UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE QUITO - CAMPUS SUR

CARRERA DE INGENIERÍA DE SISTEMAS

MENCIÓN TELEMÁTICA

IMPLEMENTACIÓN DE UN PORTAL CAUTIVO QUE PERMITA EL CONTROL DE ACCESO AL SERVICIO DE INTERNET A LOS ESTUDIANTES DEL COLEGIO SAN LUIS GONZAGA A TRAVÉS DE UNA AUTENTICACIÓN DE LOS USUARIOS MEDIANTE UN SERVICIO AAA IMPLEMENTADO EN UN SERVIDOR QUE TRABAJE CON PROTOCOLO RADIUS.

TESIS PREVIA A LA OBTENCIÓN DEL TÍTULO DE INGENIERO DE SISTEMAS

ANGEL VINICIO MALDONADO TAPIA

DIRECTOR: ING. VERÓNICA SORIA

QUITO, SEPTIEMBRE 2012

DECLARACIÓN

YO ANGEL VINICIO MALDONADO TAPIA, DECLARO BAJO JURAMENTO QUE EL TRABAJO AQUÍ DESCRITO ES DE MI AUTORÍA; QUE NO HA SIDO PRESENTADA PARA NINGÚN GRADO O CALIFICACIÓN PROFESIONAL; Y, QUE HE CONSULTADO LAS REFERENCIAS BIBLIOGRÁFICAS QUE SE INCLUYEN EN ESTE DOCUMENTO.

A TRAVÉS DE LA PRESENTE DECLARACIÓN CEDO MIS DERECHOS DE PROPIEDAD INTELECTUAL CORRESPONDIENTES A ESTE TRABAJO, A LA UNIVERSIDAD POLITÉCNICA SALESIANA, SEGÚN LO ESTABLECIDO POR LA LEY DE PROPIEDAD INTELECTUAL, POR SU REGLAMENTO Y POR LA NORMATIVIDAD INSTITUCIONAL VIGENTE.

_____

ANGEL VINICIO MALDONADO TAPIA

CERTIFICACIÓN

CERTIFICO QUE EL PRESENTE TRABAJO FUE DESARROLLADO POR EL SEÑOR ANGEL VINICIO MALDONADO TAPIA BAJO MI DIRECCIÓN.

_____

ING. VERÓNICA SORIA

AGRADECIMIENTO

A mi DIOS todo poderoso, al amor, al esfuerzo y la paciencia de mis padres, por todo el buen ejemplo y fe en mí. A la familia, que es el pilar fundamental de todo proyecto, solo me resta decir “Muchas Gracias”.

Angel Maldonado

ÍNDICE DE CONTENIDOS

ÍNDICE DE GRÁFICOS

ÍNDICE DE TABLAS

ABSTRACT

El presente proyecto describe el problema y la solución planteada para habilitar la conexión de los distintos dispositivos inalámbricos de los estudiantes del Colegio San Luis Gonzaga hacia internet.

En vista al continuo cambio en la aplicación de la tecnología dentro de la pedagogía, hace que las necesidades de conectividad, por parte de dispositivos móviles de los estudiantes hacia la red mundial de internet, como medio de consulta académica, herramienta de comunicación virtual, método complementario de aprendizaje, etc. sean más necesarias dentro de las instalaciones del Colegio San Luis Gonzaga.

Al ser este servicio un medio de acceso público y dispuesto para que se utilice con cierta cantidad de seguridad entre el estudiantado, deberá contar con un control y registro de los dispositivos que usan el servicio.

Al habilitar un servicio DHCP en una red inalámbrica se corre el riesgo de que personas ajenas a la institución obtengan la clave de acceso a la red, utilizando un software especial, y utilicen un servicio que es de uso exclusivo para el estudiantado y personal laboral del Colegio Gonzaga

El mencionado control se logrará utilizando un Portal Cautivo gestionado por el software **Chillispot**, este portal cautivo se comunicará, internamente, con el servidor **RADIUS** que es el encargado de permitir el acceso al servicio de internet mediante un “Nombre de Usuario y Password”, estas referencias del usuario son consultados en una base de datos específica diseñada en **MySQL**, la cual almacenará los registros de los usuarios en cuanto a datos de identificación y registro de utilización del portal cautivo.

Todo este proceso se logra a través de un protocolo tipo **AAA** (Autenticación, Autorización y Registro), el cual verifica la identidad del usuario, autoriza que el

usuario acceda a un servicio especificado y registra el uso que el usuario a tenido sobre el servicio.

Se plantea esta solución incluso para centralizar el espacio de uso de internet por parte de los estudiantes de la Institución. La Biblioteca Gonzalo Romero S.J. será el lugar destinado para instalar e implementar el portal cautivo con todos los componentes de hardware y software.

CAPÍTULO 1

INTRODUCCIÓN

1.1 INTRODUCCIÓN

El siguiente proyecto de tesis trabaja dentro del área de Seguridad de Redes y tiene por objetivo presentar una solución al control de acceso de los estudiantes del Colegio San Luis Gonzaga hacia la red inalámbrica que provee el servicio de Internet, siendo controlado este proceso mediante un Portal Cautivo.

El Colegio San Luis Gonzaga, en el afán de prestar el mejor servicio en cuanto a consulta de información se refiere, pretende poner a disposición de todo el estudiantado y del personal docente la conexión abierta al Internet utilizando sus computadores personales.

Debido a que la mayoría de los estudiantes y del personal docente del Colegio San Luis Gonzaga utilizarán la red inalámbrica, se deberá controlar el acceso a la misma utilizando como medio de autenticación y registro un Portal Cautivo, de este modo se evitará que personas ajenas al Colegio San Luis Gonzaga puedan utilizar los recursos de red de la institución.

En este primer capítulo se dará una breve descripción de los principales términos de referencia y conceptos con los cuales se sustentará el proyecto a realizar, por lo que estará dividido por secciones ordenadas por la jerarquización que se tiene dentro de una red informática. En el tema 1.3 se dará una breve descripción de las redes informáticas y el surgimiento de las redes inalámbricas, en el tema 1.4 se expondrá la importancia de las seguridades dentro de una red inalámbrica, en el tema 1.5 se definirá en qué consiste un Portal Cautivo y las aplicaciones que esta solución puede ofrecer.

1.2 OBJETIVOS

OBJETIVO GENERAL

Implementar un portal cautivo que permita el control de acceso al servicio de internet a los estudiantes del Colegio San Luis Gonzaga a través de la autenticación de los usuarios mediante un servicio AAA (Authenticate, Authorize, Accounting) implementado en un servidor que trabaje con protocolo RADIUS.

OBJETIVOS ESPECIFICOS

- Realizar un estudio para conocer la utilización del Internet entre los estudiantes que accedan a la red.
- Establecer las características principales con las cuales dispondrá el Portal Cautivo para el Colegio San Luis Gonzaga, tales como: diseño web de la página de inicio, funciones de validación de usuario, contabilización de uso, el control de ancho de banda, seguridades de autenticación.
- Validar autenticación por usuario-contraseña contra el servidor RADIUS.
- Integrar un servidor de bases de datos al sistema de validación.

1.3 REDES INFORMÁTICAS Y SURGIMIENTO DE LAS REDES INALÁMBRICAS

Una red informática es la interconexión física, mediante un cable o inalámbrica, de computadores o dispositivos informáticos que tiene por consigna el compartir información digital almacenada en archivos y recursos de hardware, como pueden ser: impresoras, dispositivos de almacenamiento masivo, repositorios de información digital etc. Una red informática o red de computadoras, se clasifica mediante la extensión del área a la cual cubre y ofrece su servicio de interconexión, además de la necesidad del usuario al momento de conectarse a una red informática; y según esta parametrización se divide en:

EXTENSIÓN	DEFINICIÓN	CARACTERÍSTICAS
Red de Área Local (LAN)	LAN (Local Area Network) Redes informáticas de propiedad privada: casas, campus, edificios.	✓ Se utilizan principalmente para conectar computadores personales y/o estaciones de trabajo. ✓ Operan a velocidades de 10 a 12 GBPS. ✓ Bajo retardo de transmisión. ✓ Puede utilizar varios tipos de topología de red.
Red de Área Metropolitana (MAN)	MAN (Metropolitan Area Network) Redes informáticas de propiedad pública o privada con una mayor área geográfica de cobertura: ciudades.	✓ Se utilizan principalmente para conectar oficinas cercanas, conexiones de internet y redes telefónicas. ✓ Operan a velocidades de 10 MBPS a 10 GBPS. ✓ El retardo en la transmisión oscila entre 1 y 1,5 ms. ✓ Puede utilizar varios tipos de topología de red.
Red de Área Extensa (WAN)	WAN (Wide Area Network) Redes de comunicación extendida con una gran área geográfica de cobertura: países, continentes.	✓ Se utilizan principalmente para conectar países, continentes. ✓ Operan a velocidades relativamente lentas que están entre los KBPS y MBPS. ✓ Puede utilizar varios tipos de topologías de red.

Tabla 1.1: Tipos de Redes Informáticas

Fuente: Autor de la Tesis. [cfr]

La importancia de las comunicaciones informáticas reveló algunos impedimentos en cuanto a conectividad, movilidad y seguridad dentro de una red LAN. Por lo que, posterior a la evolución a las redes cableadas se motivo a la comunicación de tipo inalámbrica.

El origen de las redes inalámbricas surgió en base a un experimento realizado por el personal de ingenieros de IBM[1] en Suiza, utilizando enlaces infrarrojos dentro de una fábrica para poder crear una red local de información. Esos resultados fueron los impulsadores de la evolución tecnológica en cuanto a las comunicaciones inalámbricas.

Posteriormente se asignó bandas de frecuencia con las cuales se pudo llegar a realizar pruebas más satisfactorias, llegando a trabajar a 1 MBPS, valor mínimo requerido por el IEEE 802 en cuanto a velocidad para que se pueda considerar como una red LAN.

La llegada de la tecnología inalámbrica (Wi-Fi) proporcionó a los distintos usuarios una manera distinta de conectarse a una red con dispositivos cada vez más versátiles y compactos.

Una red inalámbrica tiene como objetivo proporcionar a más del servicio de conectividad, la posibilidad de la comodidad al usuario que hace uso de la red, con lo que se evita el cableado excesivo y el daño de infraestructuras para poder pasar cable y medios de comunicación.

[1] IBM (International Business Machines). Empresa que fabrica y comercializa hardware, software y servicios relacionados con la informática.

Las redes inalámbricas se clasifican en varias categorías; de acuerdo al área geográfica desde la que el usuario se conecta a la red; dicha área se denomina Área de Cobertura o BSA.

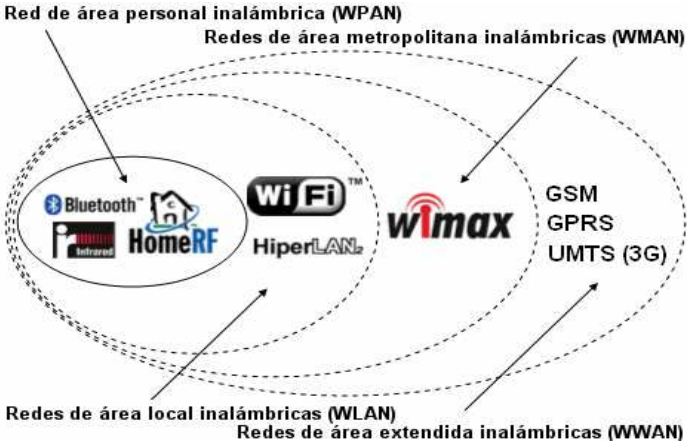


Figura 1.1: Clasificación de Redes Inalámbricas

Fuente: http://es.kioskea.net/contents/wireless/wlintro.php3

"En los últimos años las redes de área local inalámbricas (WLAN, Wireless Local Area Network) están ganando mucha popularidad, que se ve acrecentada conforme sus prestaciones aumentan y se descubren nuevas aplicaciones para ellas.
Las WLAN permiten a sus usuarios acceder a información y recursos en tiempo real sin necesidad de estar físicamente conectados a un determinado lugar."[2]

Tal ha sido el crecimiento en la utilización de las redes inalámbricas que los computadores de escritorio han sido reemplazados en un gran porcentaje con computadores y demás dispositivos móviles capaces de conectarse y compartir sus archivos y recursos con una mayor libertad de movilidad a través de una red Wi-Fi.

[2] Redes Inalámbricas, http://www.maestrosdelweb.com/editorial/redeswlan

En las redes LAN inalámbricas (WLAN), los usuarios se conectan a través de ondas de radio o luz infrarroja dentro de un espacio en el cual los equipos informáticos no están establecidos en un solo lugar y que por lo regular necesitan estar siempre conectados a una red informática o a internet.

En el caso explicito de la aplicación del Portal Cautivo, dentro del Colegio San Luis Gonzaga, se buscará que los estudiantes puedan conectarse al Internet y siempre tengan a completa disposición la información necesaria para la realización de investigaciones y proyectos educativos.

1.4 IMPORTANCIA DE LAS SEGURIDADES DENTRO DE UNA RED INALÁMBRICA

Como se ha comentado anteriormente, la utilización de las redes inalámbricas libera de las ataduras físicas en cuanto a conexión se refiere, pero la principal desventaja de utilizar una WLAN es la seguridad que esta debe tener, esto se debe a que todos los ordenadores que estén dentro de una red inalámbrica radian información y accesos a recursos informáticos ininterrumpidamente, además de que una red inalámbrica anuncia su presencia a cualquiera que este circulando dentro de su alcance o área de cobertura. Es en este punto donde se encuentra el más serio inconveniente de la utilización de una WLAN, ya que a diferencia de una red cableada, en la cual la persona que desee tener conexión deberá ubicar un acceso físico a la red interna de determinada institución, para algún intruso le bastará estar cerca del alcance de la red inalámbrica para, por un acto delictivo, obtener, manipular e incluso eliminar información perteneciente en forma privada a dicha institución o lo que pudiese ser peor, utilizar dicha red para cometer delitos informáticos hacia otras redes e instituciones.

Teniendo en cuenta todas estas premisas, se han desarrollado a lo largo de la implementación de las redes inalámbricas, métodos con los cuales poder ofrecer algún tipo de seguridad al momento de acceder a una red inalámbrica.

Entre los tipos de seguridad más utilizados en las redes inalámbricas, están los cifrados (WEP[3], WPA[4]), basados en controles de acceso mediante claves de red, lamentablemente varios estudios han comprobado que este tipo de seguridad tiene ciertas falencias en su implementación. También se puede utilizar medidas de protección como: filtrados de direcciones MAC y aplicaciones de seguridad del estándar 802.1x, mucho más robustas y confiables, ya que pueden utilizar métodos de autenticación y autorización de usuarios tal como el protocolo EAP[5] o el protocolo AAA[6] al cual se hará la mayor referencia por ser el protocolo elegido para desarrollar el presente proyecto de tesis. Este tipo de seguridades se detallarán más adelante para poder identificar ventajas e inconvenientes de cada uno.

1.5 MECANISMOS DE SEGURIDAD WLAN

1.5.1 PROTOCOLO WEP

WEP es un sistema de seguridad que utiliza la encriptación de información mediante claves para asegurarse de la confidencialidad e integridad de los datos dentro de una red inalámbrica. Este método trabaja a nivel de la Capa 2 (MAC) del Modelo OSI, usa

[3] (Wired Equivalent Privacy) Privacidad Equivalente a Cableado. Tipo de seguridad implementada para redes inalámbricas.

[4] (Wifi Protect Access) Acceso Protegido a WiFi. Mecanismo de control de acceso a una red inalámbrica.

[5] (Extensible Authentication Protocol) Protocolo de Autenticación Extensible.

[6] (Authentication, Authorization, Accounting) Autenticación, Autorización y Contabilización.

el algoritmo de encriptación RC4[7] para cifrar los datos y es soportado por la mayoría de fabricantes de productos utilizables en redes inalámbricas.

FUNCIONAMIENTO DE PROTOCOLO WEP

"RC4 trabaja de la siguiente manera:

- Existe una clave secreta compartida entre emisor y receptor que puede valer 40 ó 128 bits.
- A la trama que se enviará, se le aplica un código de integridad denominado "Integrity Check Value" (ICV) mediante el algoritmo CRC-32. Este código va a actuar como "checksum", para asegurar que lo recibido corresponde exactamente a lo que envió el emisor, es decir, la trama no ha sido modificada durante su trayecto.
- Seguidamente, se concatena la clave secreta con un número aleatorio llamado vector de inicialización, (IV) que tendrá una longitud de 24 bits. Si se utiliza siempre una misma clave para cifrar las tramas, dos tramas iguales darían lugar a tramas cifradas similares. Esto ayudaría a cualquier intruso, a descifrar los datos sin conocer la clave secreta, por ello, este vector irá cambiando en el envío de cada trama.
- El algoritmo de encriptación RC4 dispondrá de dos entradas; por una parte la clave secreta + IV (semilla) y por otra parte los datos modificados con el código de integridad (cola CRC-32). Dicho algoritmo, basándose en un proceso de XOR bit por bit generará la trama cifrada.
- Se enviara al receptor la trama cifrada (datos + CRC) junto con IV e ICV sin encriptar.

[7] RC4 es un algoritmo de cifrado en flujo que tiene una clave de 2048 bits, lo que hace que el algoritmo sea rápido y seguro. Crea bytes aleatorios a partir de la clave y hace la operación XOR byte a byte con el archivo a cifrar.

- El receptor utilizará la clave secreta que tiene compartida con el emisor, junto con el IV enviado para generar la semilla. Por medio de la semilla calculada y el algoritmo RC4 se generará la trama en claro junto con el ICV.
- Por último, el receptor calculará el ICV de los datos recibidos, y lo comparará con el ICV recibido, y si no concuerdan, descartará tanto a la trama como al emisor de la misma."[8]

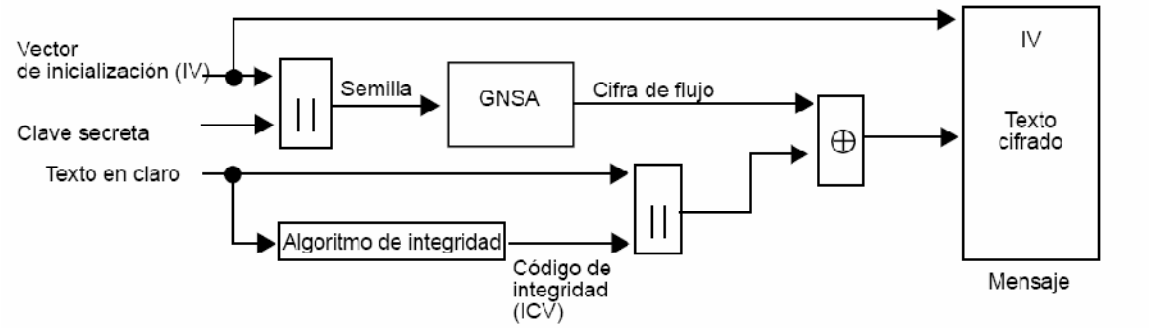


Figura 1.2: Funcionamiento de Algoritmo WEP

Fuente: [TORTOSA CERVERA]

Pero al ser un protocolo con claves fijas tiene ciertos tipos de debilidades en el vector de inicialización.

- "La clave secreta compartida entre las estaciones que intercambian tráfico tiene varios problemas:
  - Utilización de clave estática, no modificada.
  - La modificación de la clave ha de hacerse de forma manual.
  - El password del administrador es directamente la clave. Por ello la clave puede ser descubierta por ataques de diccionario.
  - Todas las estaciones que comparten PA utilizan la misma clave.

[8] [TORTOSA CERVERA, p. 11,12]

  - Por todas estas cosas resulta bastante sencillo romperla clave por fuerza bruta cuando se acumulan grandes cantidades de tráfico cifradas con la misma clave.
- El IV utilizado es de longitud insuficiente (24 bits). El número total de vectores de inicialización será entonces 2^{24}.
- Esto quiere decir, que en una red con alto tráfico (recordando que se utiliza un IV distinto por cada trama enviada) el espacio de IV distintos se agotará en un plazo relativamente corto de tiempo, de modo que la captura de dos tramas con un mismo IV no será demasiado improbable. Esto hace que con métodos estadísticos, se pueda obtener el texto en claro de una trama y con él, aplicando el algoritmo RC4, se pueda llegar a descubrir la clave secreta entre las dos estaciones.
- También existen problemas con el código de integridad (ICV). Dicho código, sirve para solucionar problemas del medio de transmisión, pero no permiten evitar modificaciones maliciosas, cambiando ciertos bits de datos y calculando los cambios del CRC-32 para mantener lo coherente."[9]

Teniendo en cuenta que el cifrado del protocolo WEP es débil y muy poco seguro, aun de este modo se puede utilizar y recomendar para redes inalámbricas dentro de oficinas pequeñas y redes domésticas que no compartan gran cantidad de información.

1.5.2 PROTOCOLO WPA

El protocolo WPA surgió como respuesta a las debilidades que ofrecía el protocolo WEP aumentando su rentabilidad y protección, esto hizo que este protocolo sea adoptado para administrarlo en usos empresariales e institucionales, ya que permite trabajar mediante autenticación de usuarios.

[9] [TORTOSA CERVERA, p. 12,13]

WPA tiene características tales como:

“

- Propuesto por los miembros de la Wi-Fi Alliance en colaboración con la IEEE.
- Basado en el protocolo para cifrado TKIP (Temporary Key IntegrityProtocol).
- La longitud de las claves pasa de 40 a 128 bits y el vector de inicialización, de 24 a 48 bits.
- La clave es generada de forma dinámica, para cada usuario, para cada sesión, y para cada paquete enviado, así como la distribución de claves, que también es realizada de forma automática.
- El mecanismo de autentificación basado en WPA emplea 802.1x/EAP”[10]

Mediante estas características, se definirá el funcionamiento de WPA en dos partes: la primera es el funcionamiento del protocolo de cifrado TKIP y la segunda es el método de autenticación en WPA.

“En primer lugar se detalla brevemente el funcionamiento del protocolo de cifrado TKIP.

- Basado en el algoritmo “Michael” para garantizar la integridad.
- Genera un bloque de 4 bytes (MIC) a partir de la dirección MAC de origen, de destino, y de los datos.
- Añade el MIC calculado a la unidad de datos a enviar.
- Posteriormente los datos se fragmentan y se les asigna un número de secuencia.
- La mezcla del número de secuencia con la clave temporal, genera la clave que será utilizada para cada fragmento.”[11]

[10] [TORTOSA CERVERA, p. 13.]

[11] [TORTOSA CERVERA, p. 14]

El método de autenticación de WPA es la mejora relevante con respecto al protocolo WEP y este trabaja bajo el estándar 802.1x, con lo que en redes de gran tamaño o empresariales utiliza un método de autenticación que se basa principalmente en tres componentes:

1. Solicitante: es el que se encuentra en la estación inalámbrica.
2. Autenticador: se encuentra en un Punto de Acceso (AP).
3. Servidor de Autenticación.

Estos tres componentes trabajan en conjunto para generar la autenticación de la siguiente manera:

- El autenticador creará un puerto de tipo lógico por cada cliente de la red.
- Al momento que el solicitante esté dentro del radio de cobertura de la red inalámbrica, el AP creará un puerto específico para el solicitante.
- Mientras el solicitante no se haya autenticado en el servidor, se le restringirá todo el tráfico de datos, dejando solamente la posibilidad que acceda al servidor de autenticación para completar el registro.

Dicha autenticación pasa por distintas fases mientras se completa el proceso de registro dentro de una red inalámbrica:

“

- El cliente envía un mensaje “EAP Start”.
- El autenticador responde con un mensaje “EAP Request Identity” para obtener la identidad del cliente.
- El solicitante responde con “EAP Response” donde indica su identificador.
- El autenticador reenviará la petición al servidor de autentificación (RADIUS).

- El cliente y servidor RADIUS pasarán a comunicarse directamente a partir de este momento, utilizando cierto algoritmo de autenticación negociado entre los dos.
- Una vez aceptada la autentificación del cliente por el servidor de autenticación, el PA (autenticador) pasará el puerto asignado inicialmente al cliente, a un estado autorizado donde no se impondrán las restricciones de tráfico existentes inicialmente."[12]

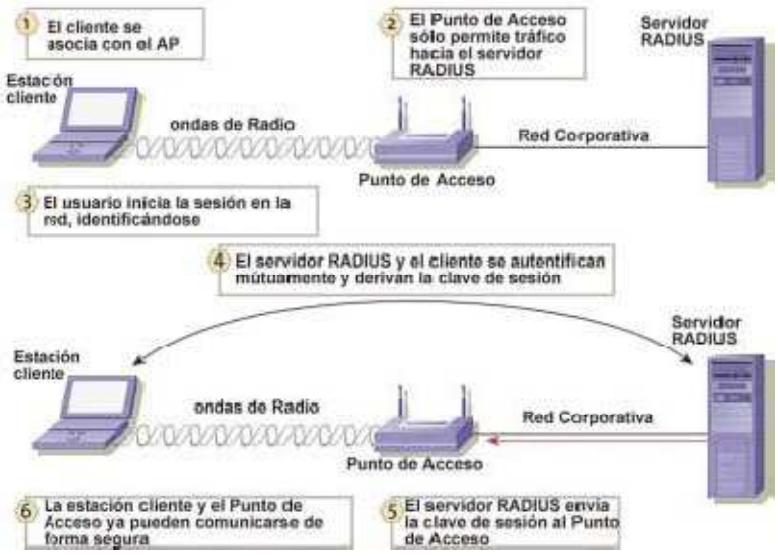


Figura 1.3: Autenticación en un Servidor RADIUS con protocolo WPA

Fuente: [TORTOSA CERVERA, p. 15]

En redes domésticas o de tamaño pequeño no es necesario que WPA pase por un servidor de autenticación, sino que más bien utiliza un protocolo llamado WPA-PSK el cual utiliza una misma clave de cifrado en todos los dispositivos, este tipo de clave tiene una longitud de 8 a 63 caracteres y se debe ingresar en cada uno de los ordenadores o dispositivos que se conecten a la red.

[12] [TORTOSA CERVERA, p. 15]

1.5.3 PROTOCOLO RADIUS

El protocolo RADIUS es un software que por sus características puede ser utilizado para generar autenticación de usuarios que acceden de forma remota a determinado servicio. Entre las aplicaciones del protocolo RADIUS están la conexión a llamadas mediante líneas conmutadas, la autenticación en redes inalámbricas 802.1x y la implementación de servicios VoIP[13].

RADIUS es un protocolo hecho por y para tres necesidades específicas:

- Autenticar (Authentication).
- Autorizar (Authorization).
- Mantener una contabilidad de uso (Accounting).

Más conocido como servicio AAA, provee de gestión a usuarios que quieren acceder a determinado recurso.

- ***"AUTENTICACIÓN (AUTHENTICATION):*** Hace referencia al proceso por el cual se determina si un usuario tiene permiso para acceder a un determinado servicio de red del que quiere hacer uso. El proceso de autenticación se realiza mediante la presentación de una identidad y unos credenciales por parte del usuario que demanda acceso.

- ***AUTORIZACIÓN (AUTHORIZATION):*** Se refiere a conceder servicios específicos (entre los que se incluye la "negación de servicio") a un determinado usuario, basándose para ello en su propia autenticación, los servicios que está solicitando, y el estado actual del sistema. Es posible configurar restricciones a la autorización de determinados servicios en

[13]VoIP Voz sobre IP, tecnología que sirve para transmitir audio por el canal clásico utilizado para transmisión de datos.

función de aspectos como, por ejemplo, la hora del día, la localización del usuario, o incluso la posibilidad o imposibilidad de realizar múltiples "logins" de un mismo usuario.

- ***REGISTRO (ACCOUNTING):*** Se refiere a realizar un registro del consumo de recursos que realizan los usuarios. El registro suele incluir aspectos como la identidad del usuario, la naturaleza del servicio prestado, y cuándo empezó y terminó el uso de dicho servicio."[14]

En el presente proyecto de tesis se utilizará al protocolo RADIUS y al servicio AAA como herramienta de implementación para el control de acceso a la red inalámbrica del Colegio San Luis Gonzaga. En los Capítulos 3 y 4 se profundizará el conocimiento y la referencia teórica de la utilización del mencionado protocolo.

Además de los métodos de seguridad ya descritos para controlar el acceso de un usuario a una red inalámbrica, existen otras técnicas con las cuales se puede asegurar la correcta utilización de este tipo de redes, dichas técnicas no precisan el cifrado de la información, sino más bien, tiene que ver con alguna configuración mínima en los equipos involucrados en la conexión.

A continuación se menciona dos técnicas que utilizan estos métodos de seguridad:

1.5.4 VPN (VIRTUAL PRIVATE NETWORK)

Las VPN son redes virtuales que se crean y configuran dentro de una red real dispuesta en un área establecida, por lo general las redes reales son de gran tamaño, por ejemplo, Internet, ATM o FrameRelay.

[14] [Universidad Politécnica de Valencia, Instalación y Configuración de un Servidor RADIUS p. 1,2,3]

“Realmente una VPN no es más que una estructura de red corporativa implantada sobre una red de recursos de carácter público, pero que utiliza el mismo sistema de gestión y las mismas políticas de acceso que se usan en las redes privadas, al fin y al cabo no es más que la creación en una red pública de un entorno de carácter confidencial y privado que permitirá trabajar al usuario como si estuviera en su misma red local.”[15]

La comunicación dentro de una VPN se establece mediante un protocolo llamado *Tunneling* que simula túneles virtuales que dan prioridad a una comunicación entre dos puntos dentro de una red pública, dicha comunicación está protegida mediante sistemas de encriptación que garantizan la confiabilidad e integridad de los paquetes de datos que viajan generalmente por una red pública, para evitar accesos no deseados a la información.

El énfasis de la seguridad que se presenta en una VPN, no solamente se limita a la utilización de protocolos de encriptación, sino que también, hace uso de técnicas de autenticación para que la comunicación dentro de la misma garantice que se la complete con los usuarios y los dispositivos correctos. La autenticación se realiza normalmente al inicio de una sesión de transmisión y luego se la realiza aleatoriamente durante el proceso de transmisión de la información.

Existen dos tipos de técnicas de encriptación que se usan en las VPN: Encriptación de clave secreta, o privada, y Encriptación de clave pública.

En la encriptación con clave secreta, todos los que participan de la transmisión vía VPN tienen conocimiento sobre una clave que propiciará el uso de la información encriptada. La desventaja de este tipo de clave es que al ser revelada se debe

[15] [GODMOL]

cambiar y difundir la nueva clave hacia todos los interesados en la información encriptada lo cual genera incomodidad y problemas de seguridad.

En la encriptación con clave pública se usan dos claves, una pública y una privada, la primera es enviada a todos los que serán partícipes de la transmisión de datos y la segunda es usada para encriptar los datos en conjunto con la clave pública que se entregó a los demás participantes. Entonces al momento de desencriptar la información se utilizará la clave privada y la clave pública de quien generó la información. La gran desventaja de este método es que todo el proceso es demasiado lento.

Tal vez la aplicación menos conocida de una VPN es la implementación de la misma sobre una red LAN, pero al mismo tiempo es una herramienta muy poderosa en cuanto a seguridad de datos se refiere dentro de una empresa. Las VPN trabajan aislando zonas, servicios o grupos de usuarios que estén ligados a una red inalámbrica (WiFi).

Este tipo de conexiones de túneles virtuales dentro de una red WiFi utilizan a los protocolos de cifrado tales como IPSEC o SSL además de los protocolos típicos de autenticación WAP, WEP, MAC Address, con lo cual aseguran que la gestión de la información o la utilización de determinados servicios sean prioritariamente seguros.

1.5.5 FILTRADO DE DIRECCIONES MAC

Este tipo de autenticación trabaja mediante el registro de la dirección física de las tarjetas de red de los equipos informáticos autorizados. Este tipo de identificación es un método adicional que se puede introducir en la seguridad de redes inalámbricas, ya que es casi imposible que una dirección MAC pueda repetirse en otra tarjeta de red. Funciona de la manera más eficiente posible dentro de ambientes pequeños y

de pocos dispositivos, ya que al manejarse en ambientes de gran cantidad de dispositivos es muy complicado llevar a cabo una correcta gestión de los equipos.

1.5.6 LIMITAR LA POTENCIA DE LA SEÑAL INALÁMBRICA DE LOS DISPOSITIVOS DE INTERCONEXIÓN

Este tipo de alternativa se puede utilizar cuando se pretenda reducir el área de cobertura de una red inalámbrica, ya que en necesidades reales lo que se busca es que ningún tipo de usuario no identificado de la red, haga un mal uso de dicha conectividad inalámbrica. Esta alternativa de seguridad en cuanto a hardware de interconexión también puede ser utilizada como un complemento a los métodos de seguridad anteriores.

Siempre es importante tener un plan de seguridad y estrategias necesarias, ya sea para cuidar información y evitar su manipulación, así también como para impedir el ingreso de intrusos a una red inalámbrica. El objetivo de la seguridad en redes informáticas inalámbricas será siempre el mismo: Precautelar la integridad, confidencialidad y disponibilidad de la información tanto como de la conectividad mediante la autenticación dentro de una red inalámbrica.

1.5.7 PORTAL CAUTIVO

Un portal cautivo, también conocido como HotSpot, es un sistema de seguridad en redes inalámbricas que pretende dar una solución al espacio de movilidad a usuarios que estén validados dentro de un servidor RADIUS[16]. Por lo general, un Portal Cautivo es una página web con la cual un usuario podrá interactuar antes de poder

[16] RADIUS es un servidor que tiene la función de autenticar a los usuarios que se conectan remotamente a una red pública o privada.

acceder a los servicios de una red inalámbrica pública o privada, con lo cual se evitará que los usuarios no deseados puedan hacer uso de los recursos de conexión.

Hay distintos tipos de Portales Cautivos, entre los cuales se pueden diferenciar a los informativos y a los restrictivos. Un Portal Cautivo de tipo informativo es aquel que presenta información de la conexión, políticas de uso de la red e incluso cierto tipo de publicidad que el administrador del Portal Cautivo quisiera que el usuario observe antes de seguir adelante con la conexión hacia el internet.

Los portales cautivos de tipo restrictivo generan un control hacia los usuarios que deseen ingresar a una determinada red. Este control se lo realiza ingresando un nombre de usuario y una contraseña; con lo cual acreditan que son usuarios registrados en un servidor RADIUS.

Según el tipo de Portal Cautivo y el tipo de usuario se puede determinar el acceso a servicios diferentes con los que podrán trabajar los beneficiarios del servicio.

Este tipo de seguridad en un Portal Cautivo trabaja mediante “Tokens” temporales gestionados por el protocolo HTTP-SSL (443/TCP). Este servicio implementa el protocolo de transferencia de hipertexto seguro (HTTPS), usando la Capa de sockets seguros (SSL) en el puerto 443 del protocolo TCP. Si se deshabilita este servicio, no se podrá iniciar ningún servicio que dependa explícitamente de él.

Para la implementación de un Portal Cautivo se puede optar por dos alternativas:

- Portal Cautivo mediante software.
- Portal Cautivo mediante hardware.

Un Portal Cautivo mediante software es un programa que crea un punto de acceso hacia internet desde un equipo informático que cuente con dos tarjetas de red, una

tarjeta para conectarse al router de Internet y la otra para conectarse a la red inalámbrica disponible.

Al ser un software, se puede instalar en una gran mayoría de computadores con arquitecturas diferentes, siempre y cuando se cuente con los requisitos necesarios de hardware para que el software funcione adecuadamente y preste el mejor de los rendimientos para el servicio propuesto. Entre algunos de los ejemplos de software para portal cautivo se tiene:

- AntamediaHotSpot
- No CatAuth
- Chillispot
- Wifidog
- FirstSpot
- mOnOwall
- Easy Captive
- Open Splash

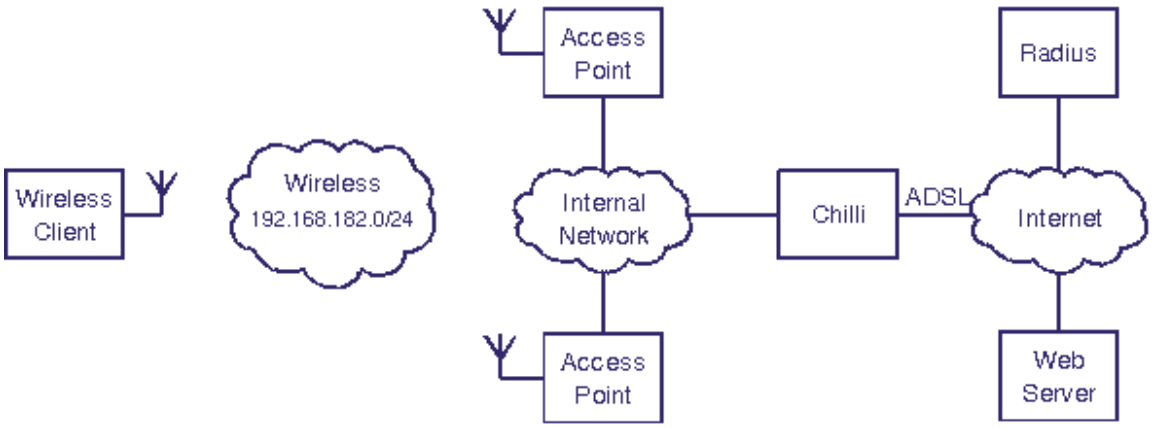


Figura 1.4: Diagrama de Portal Cautivo mediante software

Fuente: http://www.chillispot.info/index.html

La otra opción para poder configurar un Portal Cautivo es mediante hardware, este método requiere un equipo especial de conexión que permita gestionar el control de acceso a los usuarios, por lo regular este tipo de dispositivos están ubicados entre el router de salida a internet y el resto de la red informática. Internamente cuenta con un software especial para el control y funcionamiento del Portal Cautivo. Entre algunos ejemplos de dispositivos hardware que permitan administrar un Portal Cautivo están:

- OvislinkAirLive MW-2000S
- Cisco BBSM-Hotspot
- Cisco Site Selection Gateway (SSG) / Subscriber Edge Services (SESM)
- Nomadix Gateway
- Aptilo Access Gateway
- 4ipnet Hotspot Gateway
- Mikrotik
- Entre otros.

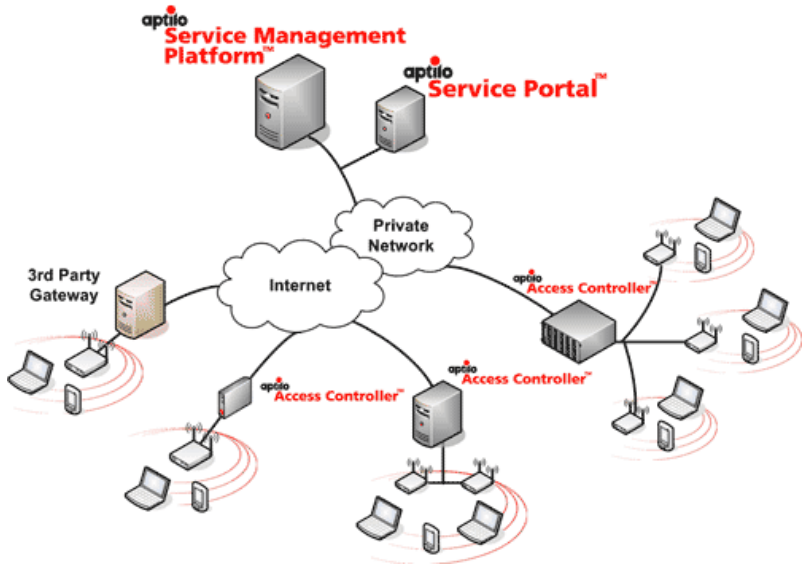


Figura 1.5: Diseño de Portal Cautivo mediante hardware con equipo Aptilo Access Gateway

Fuente: Aptilo, http:www.aptilo.com

Los dos tipos de Portales Cautivos albergan características muy similares entre las cuales se puede mencionar las siguientes:

- Se trabaja mediante una interfaz gráfica que facilita el acceso y configuración del Portal Cautivo.
- Seguridad basada en identidades.
- Configuración en base a parametrización.
- Estadísticas de uso por usuario.
- Mejor despliegue que VPN: no necesita cliente, sólo es necesario un navegador.
- Más rápidos: no hay latencia por cifrado.
- Pueden utilizar autenticación centralizada.
- Permite aplicar políticas por usuario.
- No se compromete todo el sistema.
- Muchas soluciones comerciales y libres. (Portal Cautivo mediante Software)

La diferencia establecida principalmente entre estos dos tipos de portales cautivos es el costo que tendrá el proceso de implementación, ya que en su gran mayoría, los Portales Cautivos mediante software son diseñados para instalarlos usando software de código abierto, por lo que los que son instalados mediante hardware quedan relegados a un segundo plano por que se debería adquirir dispositivos adicionales de alto costo; routers configurables, servidores de autenticación, etc.

Se muestra a continuación diferencias en escalas entre la implementación de un Portal Cautivo configurado mediante software y uno configurado mediante Hardware.

PORTAL CAUTIVO MEDIANTE:	SOFTWARE			HARDWARE		
Característica	**Bajo**	**Alto**	**Muy Alto**	**Bajo**	**Alto**	**Muy Alto**
Precio	X				X	X
Dificultad Implementación		X			X	
Estabilidad		X				X
Hardware Adicional			X	X		

Tabla 1.2: Diferencia de características entre Portal Cautivo Software y Portal Cautivo Hardware.

Fuente: Autor de la Tesis.[cfr]

En consideración, la diferencia más relevante es el precio de la implementación del portal cautivo, ya sea mediante software o mediante hardware. Al dar solamente una idea con precios que oscilan en el mercado nacional se tiene que:

PORTAL CAUTIVO		COSTO	CARACTERÍSTICAS
Software	Sw Portal Cautivo	$ 0	Sw Libre
	Sw Radius	$ 0	Sw Libre
	Sw Base de Datos	$ 0	Sw Libre
	Hw Servidor Radius	$ 300	
	Hw Access Point	$ 85	
Hardware	Sw Portal Cautivo	$ 0	Sw Propietario
	Sw Radius	$ 0	Sw Propietario / Sw Libre
	Sw Base de Datos	$ 0	Sw Propietario / Sw Libre
	Hw Portal Cautivo	$ 800 - $1500	Sw Propietario

Tabla 1.3: Comparación de precios entre Portal Cautivo Software y Portal Cautivo Hardware

Fuente: Autor de la Tesis. [cfr]

[cfr] Para la elaboración de la Tabla 1.2, se hizo referencia a [GARCÍA]

Se debe tomar en cuenta que este tipo de decisión queda a criterio de los administradores de una determinada red, ya que solamente ellos pueden establecer los requerimientos y necesidades con las que contará su sistema de seguridad.

Un Portal Cautivo maneja un proceso con el cual cumple su objetivo de autenticación de usuarios, constando de una secuencia de pasos:

1. Captura las peticiones de usuarios a una web.
2. Comprueba las credenciales de un usuario y las compara en una base de datos.
3. Autoriza el acceso al usuario dependiendo de las características de conexión y servicios necesarios.
4. Mantiene la sesión mientras está autenticado.

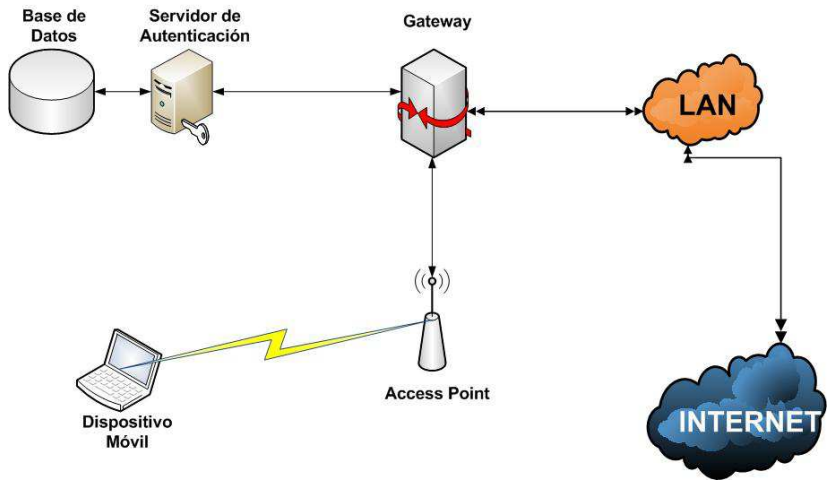


Figura 1.6: Proceso de autenticación de un Portal Cautivo

Fuente: Autor de la Tesis.

[cfr] Para la elaboración de la Tabla 1.3, se tomo en cuenta: Portal Cautivo Software; conceptos básicos sobre precios de software libre y el costo de un Access Point y un Computador con las características mencionadas en el Capitulo 3 a la fecha de su consulta. Portal Cautivo Hardware; ejemplos de precios tomados de los sitios web de los fabricantes de dispositivos hardware: 4ipnet (http://www.wifikit.co.uk/4ipnet_hotspots_s/57.htm), Cisco (http://homestore.cisco.com/en-us.htm?icid=Cisco-Home-Products-HN-MM-Shop-Cisco-Online-Store).

"El uso de un "Portal Cautivo hace que la red se vuelva funcional y dinámica. Al usar un servidor RAIDUS externo se puede centralizar la base de datos para autenticar a los clientes y así poder realizar un rommíng adecuado entre diferentes redes de la empresa. El uso de claves para los usuarios incrementa la seguridad para el acceso a la red; si un usuario ha logrado asociarse a los dispositivos inalámbricos pero no posee una cuenta creada en el servidor de autenticación, no podrá ingresar a ningún recurso, ni enviar tráfico a la red."[17]

Tomando en cuenta las consideraciones de seguridad de redes inalámbricas en las que se debe afianzar la integridad de los datos en una red y la disponibilidad de la conexión siempre que se requiera, se puede usar a un Portal Cautivo como parte de una nueva estrategia de control de acceso a una red pública o privada. La implementación de un Portal Cautivo se debe considerar cuando se requiere dar servicio de autenticación a un grupo de usuarios; por lo que el presente trabajo de tesis se enfocará en la implementación de un Portal Cautivo para los alumnos del Colegio San Luis Gonzaga que podrán gozar los beneficios de una conexión controlada y disponible con las respectivas seguridades.

[17] [CHILIQUINGA LLIVE, p. 145]

CAPÍTULO 2

ESTUDIO DE LA SITUACIÓN ACTUAL DE LA RED INALÁMBRICA DEL COLEGIO SAN LUIS GONZAGA.

A continuación se presenta un estudio respecto la situación actual de la red inalámbrica del Colegio San Luis Gonzaga en cuanto a su topología física y lógica.

Este estudio proporcionará una idea clara en la cual se podrá sustentar la implementación del Portal Cautivo, teniendo en cuenta que se puede encontrar con ciertas limitaciones a nivel físico (Hardware) que tal vez podrá ser una referencia para mejorar la infraestructura de la red de alguna manera.

A continuación se mencionará ciertos puntos clave para determinar el estado de la red inalámbrica:

- Determinar la topología física y lógica de la red inalámbrica.
- Capturar tráfico generado en la red inalámbrica.
- Identificar las seguridades establecidas dentro de la red inalámbrica.
- Determinar las áreas de cobertura (BSA) de los Routers Inalámbricos.
- Capturar la configuración de Router Inalámbrico Linksys WRT160NL.

2.1 TOPOLOGÍA FÍSICA Y LÓGICA DE LA RED INALÁMBRICA DEL COLEGIO SAN LUIS GONZAGA

Se determinará la estructura de conexión en la red de datos del Colegio San Luis Gonzaga como base para fundamentar el estudio de la situación actual de dicha red.

Se presentará a continuación el gráfico de la topología física de la red y su distribución dentro de las instalaciones del Colegio San Luis Gonzaga.

Para la representación de la topología física de la red se utilizará el software de diseño Microsoft Visio 2007, en dicha representación se incluirán los componentes activos con los que cuenta la red de datos mencionados a continuación.

CANT.	DESCRIPCIÓN DEL EQUIPO	OBSERVACIÓN
1	Router CISCO 2600 XM.	Administrable
2	Switch HP Procurve 2510 48 puertos.	Administrable
1	Switch 3COM 24 puertos	No Administrable
1	Router Inalámbrico Linksys WRT54GL	Administrable
1	Router Inalámbrico Linksys WRT160NL	Administrable
1	Access Point D-Link DWL-2100AP	No Administrable
1	Router Inalámbrico D-Link Dir 615	Administrable
1	Servidor HP Proliant	Administrable

Tabla 2.1: Componentes Activos de la Red de Datos del Colegio San Luis Gonzaga

Fuente: Autor de la Tesis.

Los dispositivos mencionados en la Tabla 2.1, se diagraman en la Figura 2.1, mostrando la topología física de la red del Colegio San Luis Gonzaga.

La distribución de todos los dispositivos de la red hace que la topología física de la misma sea de tipo Estrella con su variante Estrella Extendida, ya que todos los ordenadores no están conectados directamente a un dispositivo central sino a varios puntos subcentrales.

El router CISCO, salida a la conexión de internet, está conectado a un switch HP Procurve 2510 principal, de este se conectan dos switch adicionales los cuales dan conectividad al área administrativa; switch 3COM 4226T, y a un laboratorio informático; switch HP Procurve 2510.

Del switch principal se establece una conexión con dos routers inalámbricos, uno de marca Linksys WRT54GL y uno de marca D-Link DIR 615, los cuales ofrecen una conectividad inalámbrica al sector sur y norte de las instalaciones del Colegio San Luis Gonzaga respectivamente, esta conexión a los routers inalámbricos se da a través de fibra óptica para el sector sur del Colegio San Luis Gonzaga y mediante cable UTP para el sector norte. El router inalámbrico Linksys wrt54g del sector sur da conexión a dos switch 3COM los cuales conectan los dispositivos de Biblioteca y Sala de Profesores, además, da conexión a la Casa Comunidad mediante la conexión de un Access Point D-Link DWL-2100AP.

En cuanto a la topología lógica de la red de datos del Colegio San Luis Gonzaga, se puede mencionar que según su funcionamiento y configuración está definida dentro de la topología Bus Estrella ya que se utiliza el par trenzado como medio de transmisión por defecto. El gráfico de la topología física y listado de los protocolos utilizados en la red del Colegio San Luis Gonzaga se detalla a continuación:

PROTOCOLO	DESCRIPCION
Ethernet	• Protocolo más sencillo y de bajo costo que se puede implementar en una red de datos. • Utiliza una topología lógica punto a punto. • Trabaja a una velocidad de 10 Mbps (Ethernet), 100 Mbps (Fast Ethernet), 1000 Mbps (Giga Ethernet).

Tabla 2.2: Protocolos de red utilizados en la Red del Colegio San Luis Gonzaga

Fuente: Autor de la Tesis.

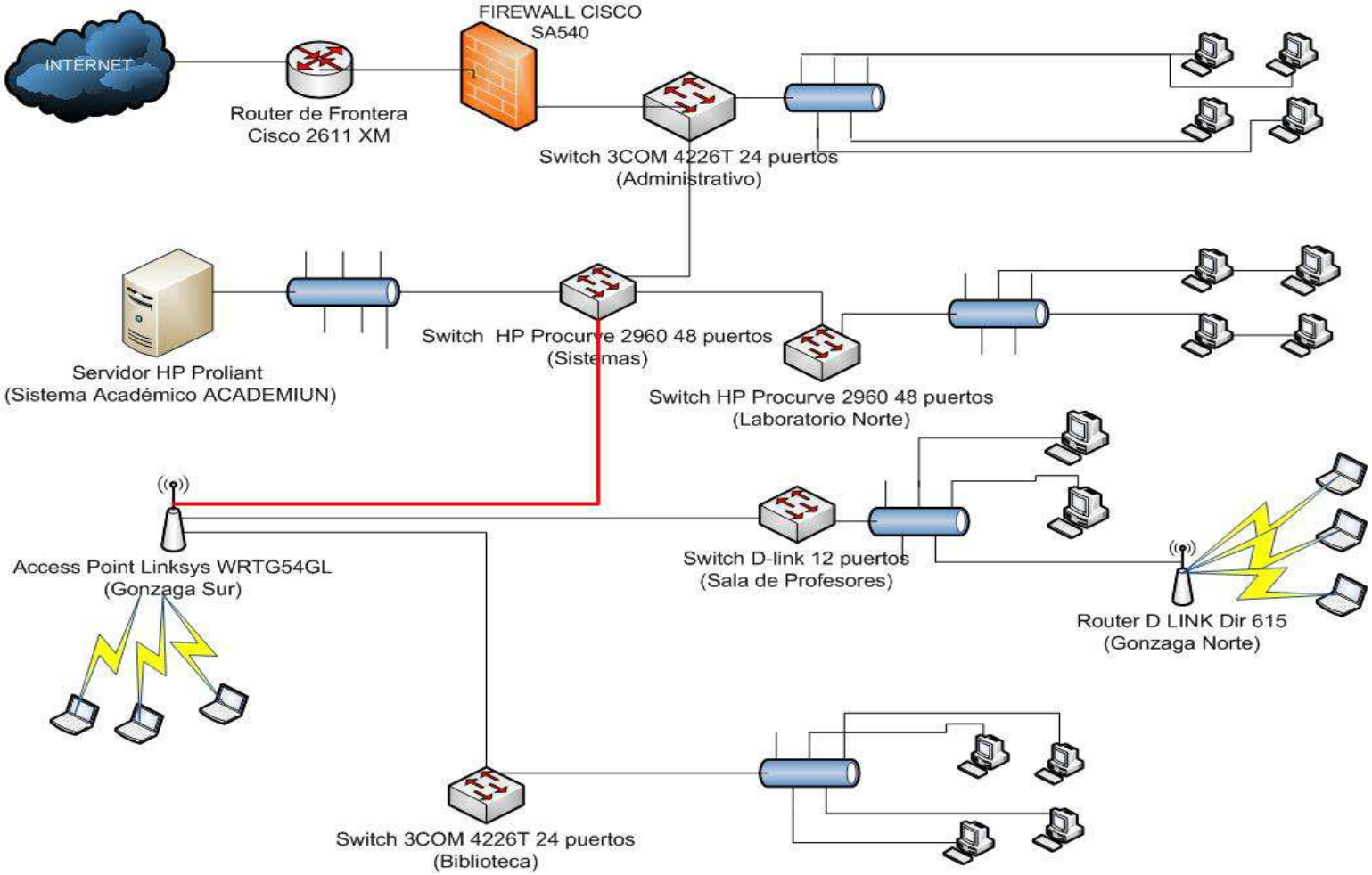


Figura 2.1: Topología Física de la Red del Colegio San Luis Gonzaga.

Fuente: Autor de la Tesis.

2.2 CAPTURA DE TRÁFICO GENERADO EN LA RED INALÁMBRICA

Se capturará tráfico de datos dentro de la red inalámbrica para analizarlos de tal manera que sean un referente en cuanto a la seguridad que se podrá aplicar como parte activa de la implementación del Portal Cautivo. Para la captura y análisis de información se utilizará el software *WireShark*[18] el cual se ejecutará sobre la plataforma Windows XP.

Los paquetes capturados a través del software Wireshark son del día miércoles 9 de septiembre del 2011. Los datos capturados muestran los protocolos con los cuales están haciendo relación y en el siguiente gráfico se detallarán los porcentajes de los protocolos utilizados.

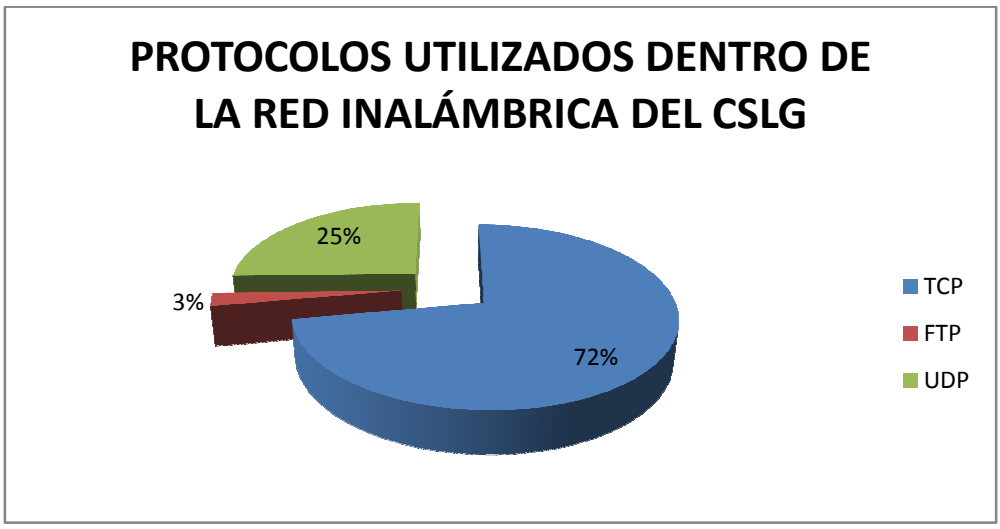


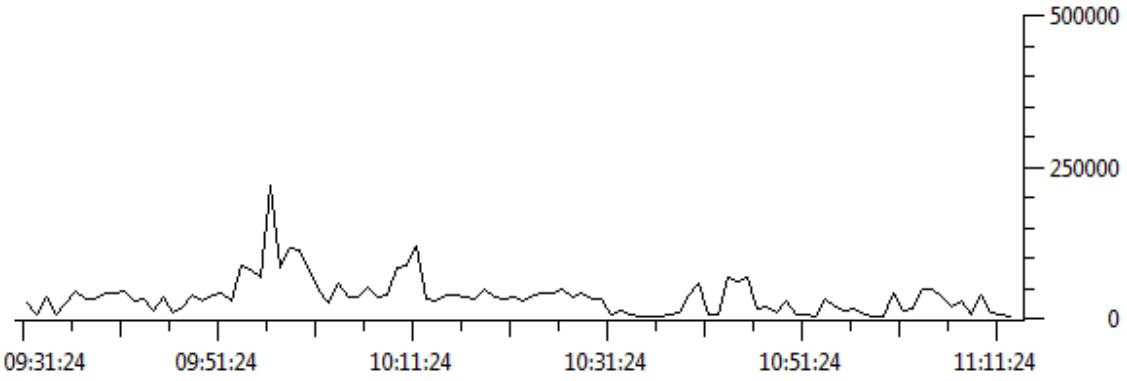
Figura 2.2: Análisis de Protocolos capturados en la red inalámbrica del Colegio San Luis Gonzaga.

Fuente: Autor de la Tesis.

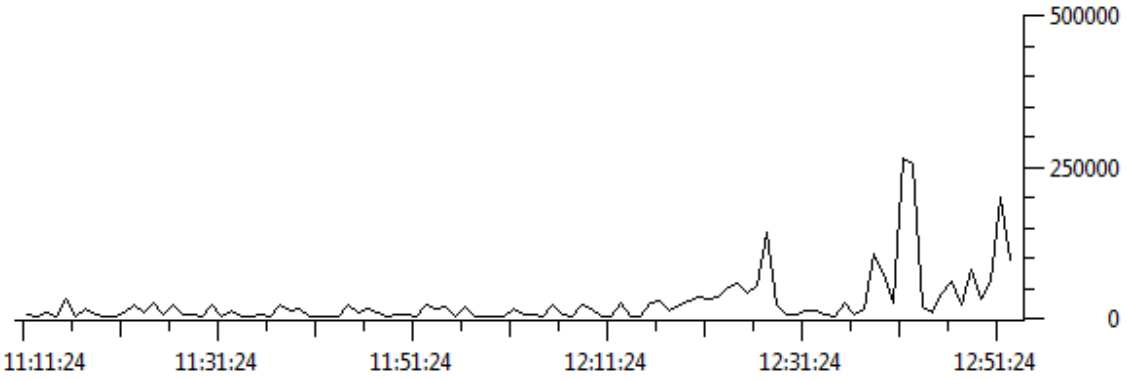
[18]Wireshark es un analizador de protocolos de red para Windows y Unix el cual permite examinar la información de una red en tiempo real. Además permite obtener información detallada de cada paquete de datos, mostrándolos incluso por tipo (UDP, TCP, ICMP, IPX, etc.).

Durante este periodo de tiempo se capturaron alrededor de 232939 paquetes en donde el 64% son de petición web es decir paquetes con protocolo TCP a través del puerto 80, por lo tanto esos son los paquetes que se tomarán mayoritariamente en cuenta para dicho análisis.

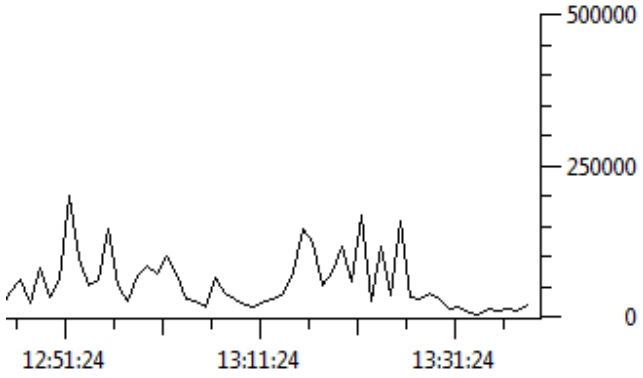
Se presenta a continuación los gráficos correspondientes al análisis de los paquetes capturados dentro del periodo de tiempo establecido entre las 09 horas 30 minutos de la mañana hasta las 13 horas 31 minutos en la tarde, con esto se representa visualmente la hora en la cual las peticiones web son más frecuentes a través de una comparación de cantidades de Bytes transmitidos, mostrando los siguientes resultados:



(A)



(B)



(C)

Figura 2.3: Análisis de cantidad de Bytes en la red del Colegio San Luis Gonzaga

(A): Cantidad de Bytes capturados entre 9:31am y 11:11 am

(B): Cantidad de Bytes capturados entre 11:11am y 12:51 pm

(C): Cantidad de Bytes capturados entre 12:51pm y 13:31 pm

Fuente: Autor de la Tesis.

2.3 SEGURIDADES ESTABLECIDAS DENTRO DE LA RED INALÁMBRICA

La seguridad con la que cuenta la red inalámbrica del Colegio San Luis Gonzaga es solamente la provista por una clave WEP de 64 bits con 10 dígitos Hexadecimales, por lo que representa una gran desventaja en cuanto a la posibilidad de plagio de la clave WEP por parte de gente externa a la institución que pueda hacer un uso malintencionado o desmedido de los recursos de red.

Teniendo en cuenta la clasificación de una clave de tipo WEP se mencionará sus características:

2.3.1 CLAVE WEP DE SISTEMA ABIERTO: Este tipo de sistema de seguridad no exige que un posible usuario de una red inalámbrica tenga que identificarse hacia el Punto de Red durante la autenticación. Así que no importa si el usuario no cuenta con una clave WEP, sino que puede

verificarse primero en el Punto de Acceso y luego podrá intentar tener éxito en la conexión. Luego de este proceso se puede utilizar la clave WEP como un método de cifrado para paquetes de datos. Obviamente se deberá tener las claves correctas.

2.3.2 CLAVE WEP COMPARTIDA: Este método se utiliza para autenticar a un usuario dentro de una red inalámbrica, y puede ser implementado mediante cuatro fases:

1. La estación cliente envía una petición de autenticación al Punto de Acceso.
2. El punto de acceso envía de vuelta un texto modelo.
3. El cliente tiene que cifrar el texto modelo usando la clave WEP ya configurada, y reenviarlo al Punto de Acceso en otra petición de autenticación.
4. El Punto de Acceso descifra el texto codificado y lo compara con el texto modelo que había enviado. Dependiendo del éxito de esta comparación, el Punto de Acceso envía una confirmación o una denegación. Después de la autenticación y la asociación, WEP puede ser usado para cifrar los paquetes de datos.

En los Puntos de Acceso con los que cuenta el Colegio San Luis Gonzaga, se tiene un tipo de clave WEP de sistema Abierto, de este modo es necesario que el usuario de la red inalámbrica cuente con la clave correcta.

Además las direcciones IP establecidas para la conectividad son estáticas, dejando a un lado las direcciones IP dinámicas, las cuales aportarían a que un usuario externo a la institución cuente con un ingreso mucho más sencillo a la red inalámbrica.

El router inalámbrico que provee de servicio de red, nunca se desconecta ni se apaga, por lo que está en permanente visibilidad para los intrusos que quisieran conectarse a la red de datos del Colegio San Luis Gonzaga.

Teniendo en cuenta la facilidad con la que gente ajena a la institución educativa puede obtener la clave de seguridad WEP, por medio de software especializado en quebrantar dicha restricción, la clave de acceso a la red es cambiada cada tres meses, como promedio, procurando mantener segura la red de la Institución Educativa, por este motivo se opta por implementar otro sistema de seguridad el cual permita la autenticación de usuarios, proporcionando un nivel mayor de seguridad al acceso a los recursos de la red.

2.4 ÁREA DE COBERTURA DE LOS ACCESS POINT (BSA)

"Área de servicio básico (BSA) es la zona donde se comunican las estaciones de una misma BSS, se definen dependiendo del medio Movilidad este es un concepto importante en las redes 802.11, ya que lo que indica es la capacidad de cambiar la ubicación de los terminales, variando la BSS. La transición será correcta si se realiza dentro del mismo ESS en otro caso no se podrá realizar. Límites de la red los límites de las redes 802.11 son difusos ya que pueden solaparse diferentes BSS. "[19]

Teniendo en cuenta que se considera a BSS (Basic Service Set) como el área de cobertura básica dentro de una red y dentro de la cual se pueden agrupar una cantidad de estaciones móviles que se comuniquen entre sí pudiendo interpretarse dentro de dos tipos de intercomunicación:

1. Independientes: cuando los dispositivos se intercomunican directamente.

[19][ENCISO ROCHA]

2. Infraestructura: cuando los dispositivos se intercomunican a través de un punto de acceso (redes inalámbricas).

Se debe trabajar con ciertos parámetros cuando se utilizan dispositivos de comunicación inalámbricos, este tipo de disposiciones van de acuerdo a la ubicación geográfica, a los obstáculos visibles, los factores climáticos e inclusive la temperatura puede afectar a la normal propagación de la señal de radio frecuencia.

Se puede definir el área de cobertura dependiendo de la frecuencia con la que trabaja el dispositivo inalámbrico y la cantidad de decibeles que puedan emitir las antenas acopladas a dichos dispositivos. En la siguiente tabla se muestra una comparación entre los parámetros antes mencionados y el posible espacio de cobertura entre esos parámetros.

FRECUENCIA	DECIBELES DE ANTENA	DISTANCIA
2,4 GHz	100dBi	1 Km
	120dBi	10 Km
	140dBi	100 Km
5 GHz	108dBi	1 Km
	128dBi	10 Km
	148dBi	100 Km

Tabla 2.3: Distancia a cubrir en relación a frecuencia y decibeles.

Fuente: [NAVARRO]

Se mencionará a continuación una tabla en la cual se enlista los distintos canales con sus respectivas propiedades y en las regiones en las cuales trabajan.

IDENTIFICADOR DE CANAL	FRECUENCIA EN MHZ	DOMINIOS REGULADORES				
		América (-A)	EMEA (-E)	Israel (-I)	China (-C)	Japón (-J)
1	2,412	X	X	-	X	X
2	2,417	X	X	-	X	X
3	2,422	X	X	X	X	X
4	2,427	X	X	X	X	X
5	2,432	X	X	X	X	X
6	2,437	X	X	X	X	X
7	2,442	X	X	X	X	X
8	2,447	X	X	X	X	X
9	2,452	X	X	X	X	X
10	2,457	X	X	-	X	X
11	2,462	X	X	-	X	X
12	2,467	-	X	-	-	X
13	2,472	-	X	-	-	X
14	2,484	-	-	-	-	X

Tabla 2.4: Identificadores de canales, frecuencias centrales, y dominios reguladores para cada canal usado por IEEE 802.11b e IEEE 802.11g.

Fuente: [DURÁN]

En donde los dispositivos inalámbricos, más comunes a mencionar, son access point o routers inalámbricos, dichos dispositivos trabajan mediante canales de radio frecuencia que en su gran mayoría están en el rango de 2,4 GHz los cuales se encuentran registrados en las frecuencias de la región del Continente Americano.

CANAL	FRECUENCIA (GHZ)
1	2,412
2	2,417
3	2,422
4	2,427
5	2,432
6	2,437
7	2,442
8	2,447
9	2,452
10	2,457
11	2,462
12	2,467
13	2,472
14	2,484

Tabla 2.5: Canales de Radio Frecuencia y Valores de GHz.

Fuente: [NAVARRO]

Dentro de las instalaciones del Colegio San Luis Gonzaga se dispone de dos routers inalámbricos activos y un router inalámbrico inactivo, contando con las siguientes características técnicas:

(A)

Velocidad: 54 Mbps

Tipo de puertos: 4 LAN RJ45, 1 WAN RJ45

Estándar: 802.11 b y g

Frecuencia: 2,4 GHz (Canal Americano)

Antenas: 2 de 7dBi

Configuración: Administrable - Activo

(B)

Velocidad: Hasta 300 Mbps

Tipo de puertos: 4 LAN RJ45, 1 WAN RJ45

Estándar: 802.11 b, g y n

Frecuencia: 2,4 GHz (Canal Americano)

Antenas: 2 de 2dBi

Configuración: Administrable - Activo

(C)

Velocidad: Hasta 300 Mbps

Tipo de puertos: 4 LAN RJ45, 1 WAN RJ45

Estándar: 802.11 b, g y n

Frecuencia: 2,4 GHz (Canal Americano)

Antenas: 2 de 5dBi

Configuración: Administrable - Inactivo

Figura 2.4: Router Inalámbricos disponibles en el Colegio San Luis Gonzaga

(A) Router Linksys WRT54GL

(B) Router D-Link Dir 615

(C) Router Linksys WRT160NL

Por lo que al hacer una referencia a las Tablas 2.4 y 2.5 se obtiene que el BSA teórico es de 0,02 Km en el router D-Link DIR 615 y de 0,07 Km en el router Linksys WRT54G y WRT160NL, en línea de vista. Cubriendo dos sectores dentro de las instalaciones del Colegio San Luis Gonzaga designados como Gonzaga-Norte y Gonzaga-Sur, respectivamente.

En el siguiente gráfico, se muestra de manera visual la ubicación de los routers inalámbricos activos dentro de las instalaciones del Colegio San Luis Gonzaga.

Figura 2.5: Routers Inalámbricos Colegio San Luis Gonzaga.

Fuente: Google Earth.

La Figura 2.5 se la obtuvo utilizando la aplicación Google Earth, mostrando la distribución física y real del área total del Colegio San Luis Gonzaga.

Figura 2.6: BSA de las redes inalámbricas Colegio San Luis Gonzaga.

Fuente: Autor de la Tesis.

La Figura 2.6 se la realizó en base a los datos obtenidos mediante software tipo SiteSurvey de verificación de intensidad de señal inalámbrica (inSSIDer 2.0).

Con los gráficos obtenidos con inSSIDer 2.0 y un cálculo realizado en Autocad 2009, se determina como resultado que el área y perímetro que cubre cada uno de las redes inalámbricas dentro de las instalaciones del Colegio San Luis Gonzaga son:

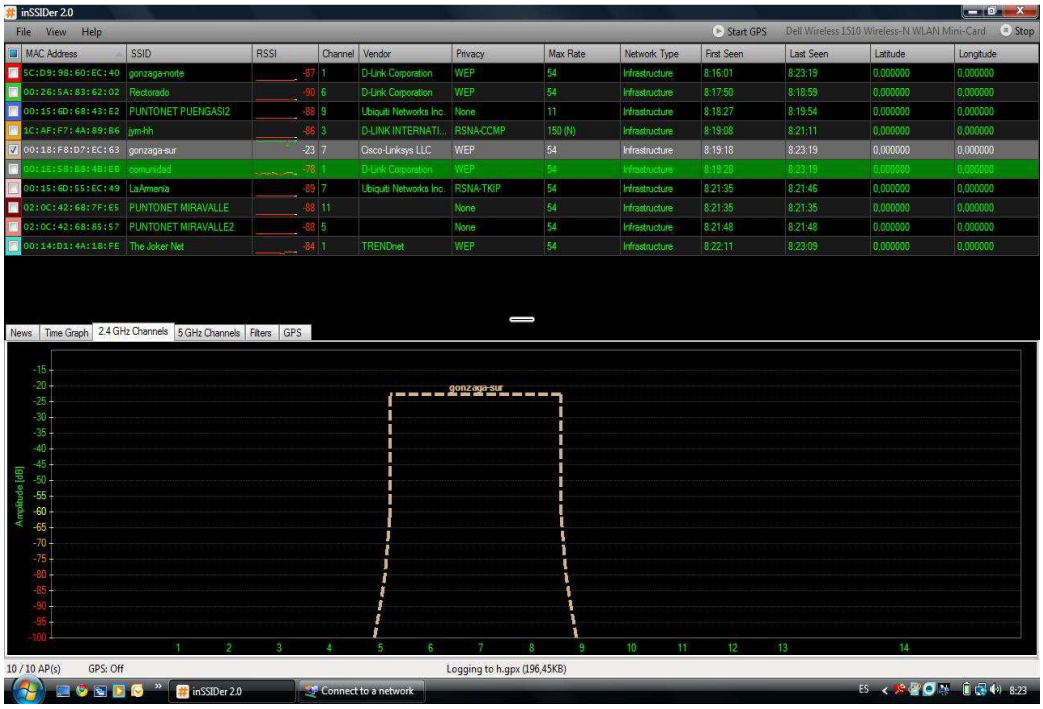
- Gonzaga-Norte
    - Área: 4714,22 m^2
    - Perímetro: 294,58 m

- Gonzaga-Sur
    - Área: 4036,05 m^2
    - Perímetro: 273,52 m

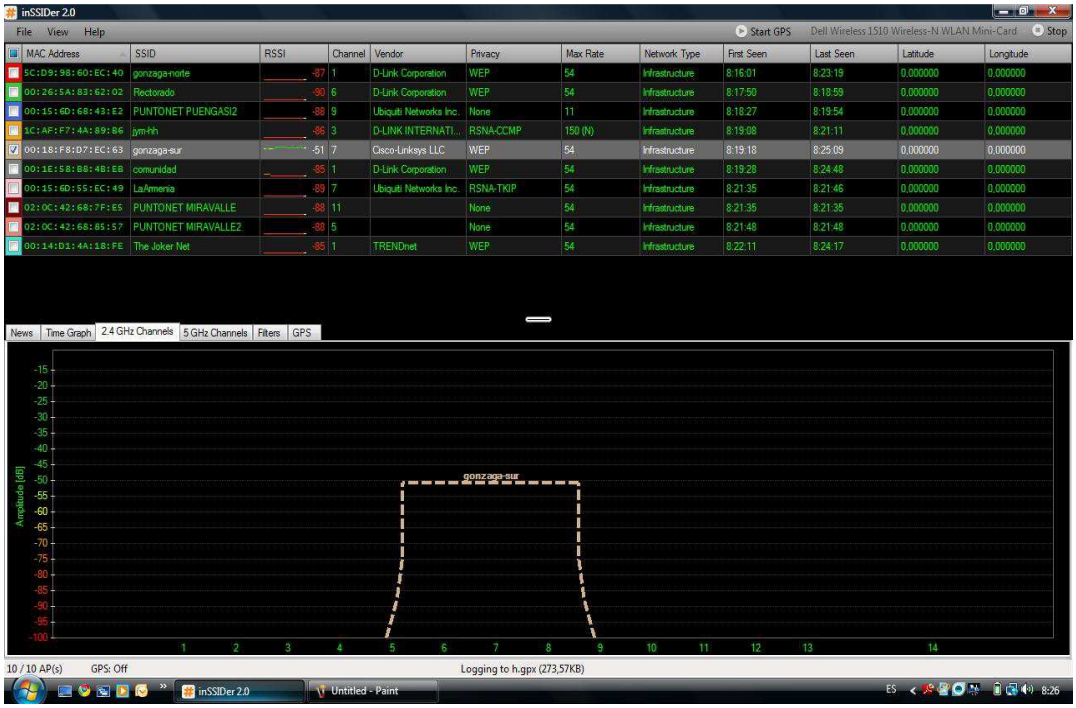
Se acota que los gráficos mostrados a continuación son una referencia de la distancia de cobertura de cada uno de los routers inalámbricos, y fueron obtenidos en condiciones ideales, es decir, sin ningún usuario conectado a la red de datos del Colegio San Luis Gonzaga, y además, monitoreados en línea de vista, sin ningún objeto que haga interferencia entre el router inalámbrico y el computador con el software sitesurvey, por lo que es de total notoriedad la intensidad de señal con la que un usuario de la red de datos del Colegio San Luis Gonzaga podría conectarse dependiendo de la distancia hacia el dispositivo de red inalámbrico.

Para los dos routers de marca Linksys se tiene referencia de los mismos gráficos de medición ya que poseen configuraciones similares en cuanto a software y hardware, diferenciados solamente por el modelo y año de producción.

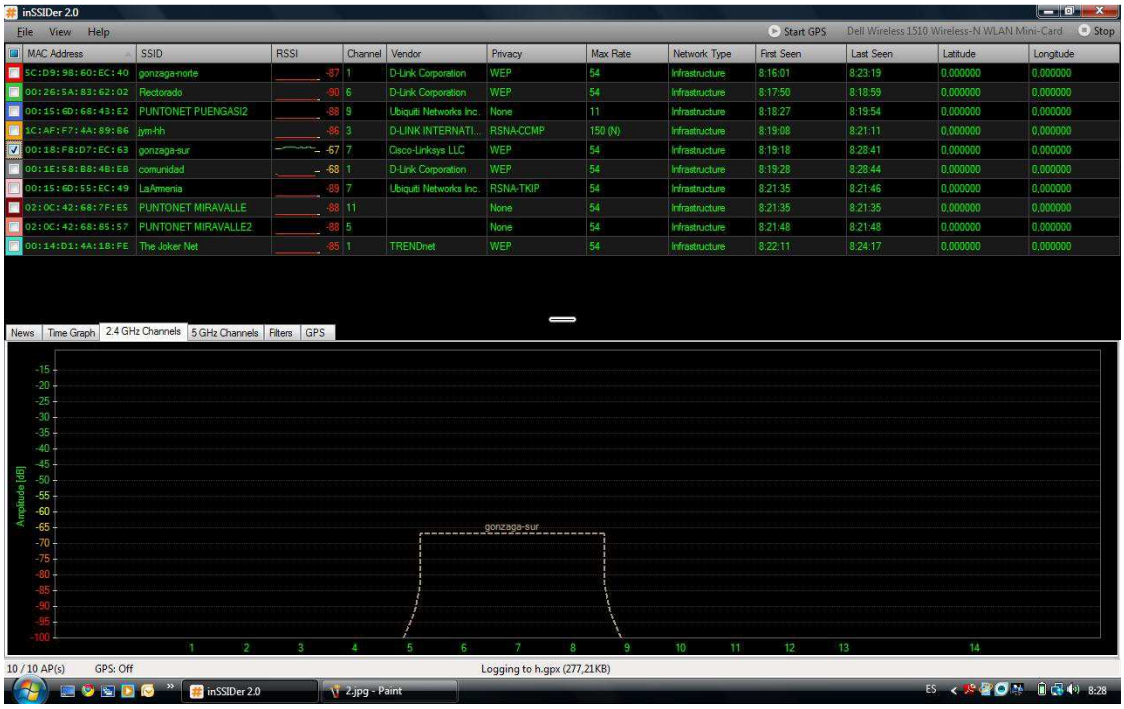
Se presenta a continuación las mediciones obtenidas en base a la utilización de software SiteSurvey para las redes Gonzaga-Norte y Gonzaga-Sur.


inSSIDer 2.0
File View Help
Start GPS
Dell Wireless 1510 Wireless-N WLAN Mini-Card
Stop
MAC Address | SSID | RSSI | Channel | Vendor | Privacy | Max Rate | Network Type | First Seen | Last Seen | Latitude | Longitude
5C:D9:98:60:EC:40 | gonzaga-norte | -87 | 1 | D-Link Corporation | WEP | 54 | Infrastructure | 8:16:01 | 8:23:19 | 0,000000 | 0,000000
00:26:5A:83:62:02 | Rectorado | -90 | 6 | D-Link Corporation | WEP | 54 | Infrastructure | 8:17:50 | 8:18:59 | 0,000000 | 0,000000
00:15:6D:68:43:E2 | PUNTONET PUENGASI2 | -88 | 9 | Ubiquiti Networks Inc. | None | 11 | Infrastructure | 8:18:27 | 8:19:54 | 0,000000 | 0,000000
1C:AF:F7:4A:89:86 | jym-hh | -86 | 3 | D-LINK INTERNATI... | RSNA-CCMP | 150 (N) | Infrastructure | 8:19:08 | 8:21:11 | 0,000000 | 0,000000
00:18:F8:D7:EC:63 | gonzaga-sur | -23 | 7 | Cisco-Linksys LLC | WEP | 54 | Infrastructure | 8:19:18 | 8:23:19 | 0,000000 | 0,000000
00:1E:58:B8:4B:EB | comunidad | -76 | 1 | D-Link Corporation | WEP | 54 | Infrastructure | 8:19:28 | 8:23:19 | 0,000000 | 0,000000
00:15:6D:55:EC:49 | LaArmenia | -89 | 7 | Ubiquiti Networks Inc. | RSNA-TKIP | 54 | Infrastructure | 8:21:35 | 8:21:46 | 0,000000 | 0,000000
02:0C:42:68:7F:E5 | PUNTONET MIRAVALLE | -88 | 11 | | None | 54 | Infrastructure | 8:21:35 | 8:21:35 | 0,000000 | 0,000000
02:0C:42:68:85:57 | PUNTONET MIRAVALLE2 | -88 | 5 | | None | 54 | Infrastructure | 8:21:48 | 8:21:48 | 0,000000 | 0,000000
00:14:D1:4A:18:FE | The Joker Net | -84 | 1 | TRENDnet | WEP | 54 | Infrastructure | 8:22:11 | 8:23:09 | 0,000000 | 0,000000
News Time Graph 2.4 GHz Channels 5 GHz Channels Filters GPS
gonzaga-sur
Amplitude [dB]
10 / 10 AP(s)
GPS: Off
Logging to h.gpx (196,45KB)
inSSIDer 2.0
Connect to a network
ES
8:23

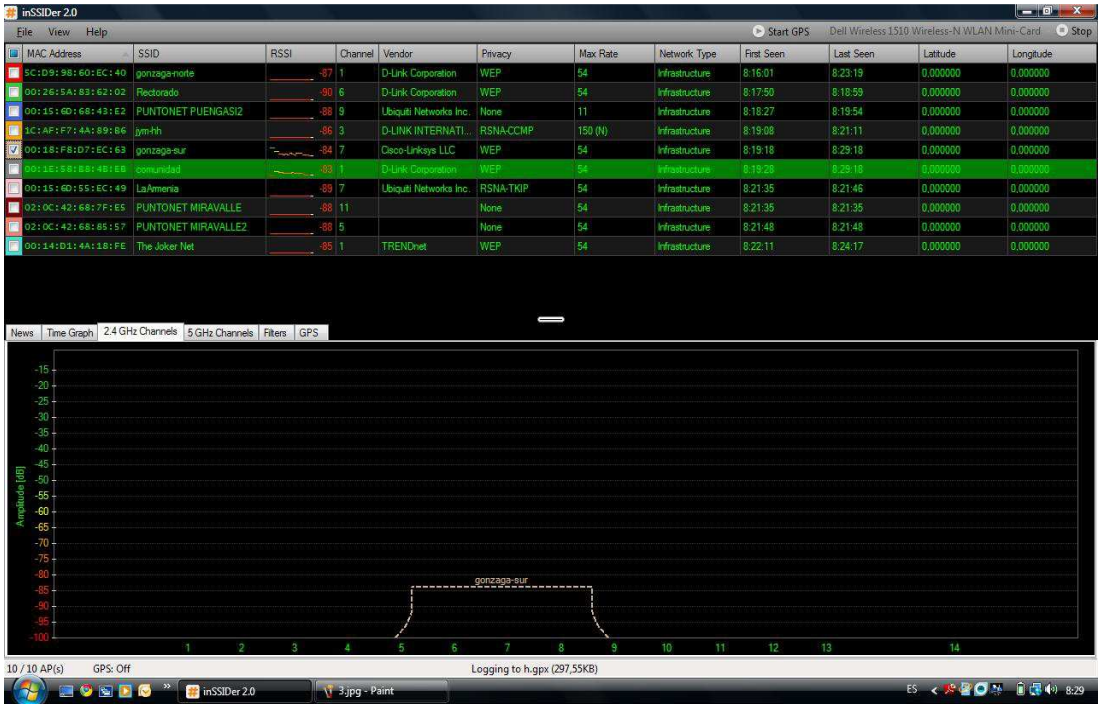
(A)


inSSIDer 2.0
File View Help
Start GPS
Dell Wireless 1510 Wireless-N WLAN Mini-Card
Stop
MAC Address | SSID | RSSI | Channel | Vendor | Privacy | Max Rate | Network Type | First Seen | Last Seen | Latitude | Longitude
5C:D9:98:60:EC:40 | gonzaga-norte | -87 | 1 | D-Link Corporation | WEP | 54 | Infrastructure | 8:16:01 | 8:23:19 | 0,000000 | 0,000000
00:26:5A:83:62:02 | Rectorado | -90 | 6 | D-Link Corporation | WEP | 54 | Infrastructure | 8:17:50 | 8:18:59 | 0,000000 | 0,000000
00:15:6D:68:43:E2 | PUNTONET PUENGASI2 | -88 | 9 | Ubiquiti Networks Inc. | None | 11 | Infrastructure | 8:18:27 | 8:19:54 | 0,000000 | 0,000000
1C:AF:F7:4A:89:86 | jym-hh | -86 | 3 | D-LINK INTERNATI... | RSNA-CCMP | 150 (N) | Infrastructure | 8:19:08 | 8:21:11 | 0,000000 | 0,000000
00:18:F8:D7:EC:63 | gonzaga-sur | -51 | 7 | Cisco-Linksys LLC | WEP | 54 | Infrastructure | 8:19:18 | 8:25:09 | 0,000000 | 0,000000
00:1E:58:B8:4B:EB | comunidad | -85 | 1 | D-Link Corporation | WEP | 54 | Infrastructure | 8:19:28 | 8:24:48 | 0,000000 | 0,000000
00:15:6D:55:EC:49 | LaArmenia | -89 | 7 | Ubiquiti Networks Inc. | RSNA-TKIP | 54 | Infrastructure | 8:21:35 | 8:21:46 | 0,000000 | 0,000000
02:0C:42:68:7F:E5 | PUNTONET MIRAVALLE | -88 | 11 | | None | 54 | Infrastructure | 8:21:35 | 8:21:35 | 0,000000 | 0,000000
02:0C:42:68:85:57 | PUNTONET MIRAVALLE2 | -88 | 5 | | None | 54 | Infrastructure | 8:21:48 | 8:21:48 | 0,000000 | 0,000000
00:14:D1:4A:18:FE | The Joker Net | -85 | 1 | TRENDnet | WEP | 54 | Infrastructure | 8:22:11 | 8:24:17 | 0,000000 | 0,000000
News Time Graph 2.4 GHz Channels 5 GHz Channels Filters GPS
gonzaga-sur
Amplitude [dB]
10 / 10 AP(s)
GPS: Off
Logging to h.gpx (273,57KB)
inSSIDer 2.0
Untitled - Paint
ES
8:26

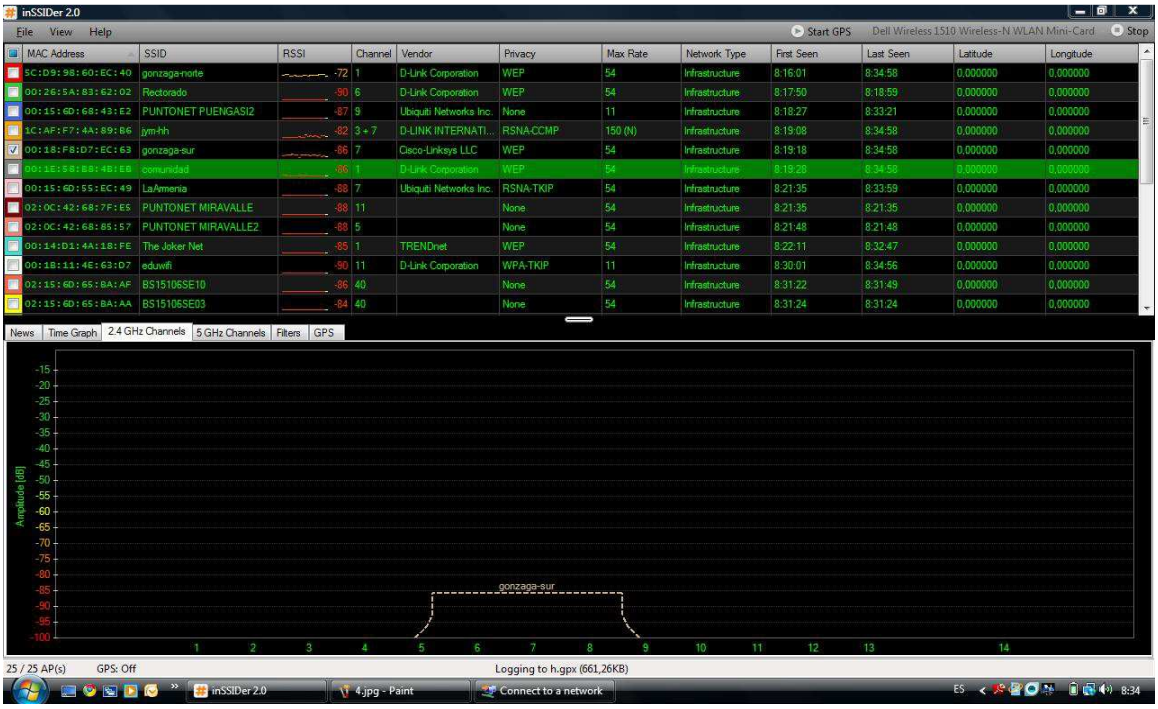
(B)


inSSIDer 2.0
File View Help
Start GPS
Dell Wireless 1510 Wireless-N WLAN Mini-Card
Stop
MAC Address | SSID | RSSI | Channel | Vendor | Privacy | Max Rate | Network Type | First Seen | Last Seen | Latitude | Longitude
5C:D9:98:60:EC:40 | gonzaga-norte | -87 | 1 | D-Link Corporation | WEP | 54 | Infrastructure | 8:16:01 | 8:23:19 | 0,000000 | 0,000000
00:26:5A:83:62:02 | Rectorado | -90 | 6 | D-Link Corporation | WEP | 54 | Infrastructure | 8:17:50 | 8:18:59 | 0,000000 | 0,000000
00:15:6D:68:43:E2 | PUNTONET PUENGASI2 | -88 | 9 | Ubiquiti Networks Inc. | None | 11 | Infrastructure | 8:18:27 | 8:19:54 | 0,000000 | 0,000000
1C:AF:F7:4A:89:86 | jym-hh | -86 | 3 | D-LINK INTERNATI... | RSNA-CCMP | 150 (N) | Infrastructure | 8:19:08 | 8:21:11 | 0,000000 | 0,000000
00:18:F8:D7:EC:63 | gonzaga-sur | -67 | 7 | Cisco-Linksys LLC | WEP | 54 | Infrastructure | 8:19:18 | 8:28:41 | 0,000000 | 0,000000
00:1E:58:B8:4B:EB | comunidad | -68 | 1 | D-Link Corporation | WEP | 54 | Infrastructure | 8:19:28 | 8:28:44 | 0,000000 | 0,000000
00:15:6D:55:EC:49 | LaArmenia | -89 | 7 | Ubiquiti Networks Inc. | RSNA-TKIP | 54 | Infrastructure | 8:21:35 | 8:21:46 | 0,000000 | 0,000000
02:0C:42:68:7F:E5 | PUNTONET MIRAVALLE | -88 | 11 | | None | 54 | Infrastructure | 8:21:35 | 8:21:35 | 0,000000 | 0,000000
02:0C:42:68:85:57 | PUNTONET MIRAVALLE2 | -88 | 5 | | None | 54 | Infrastructure | 8:21:48 | 8:21:48 | 0,000000 | 0,000000
00:14:D1:4A:18:FE | The Joker Net | -85 | 1 | TRENDnet | WEP | 54 | Infrastructure | 8:22:11 | 8:24:17 | 0,000000 | 0,000000
News Time Graph 2.4 GHz Channels 5 GHz Channels Filters GPS
Amplitude [dB]
gonzaga-sur
10 / 10 AP(s) GPS: Off
Logging to h.gpx (277,21KB)
inSSIDer 2.0
2.jpg - Paint
ES 8:28

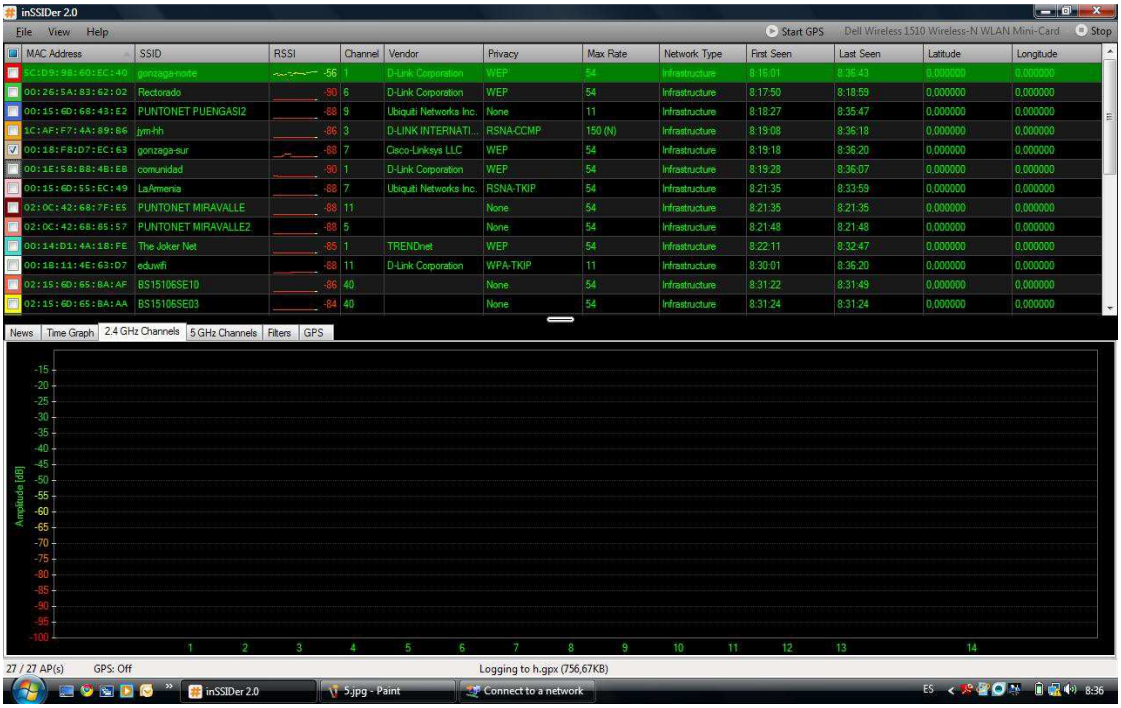
(C)


inSSIDer 2.0
File View Help
Start GPS
Dell Wireless 1510 Wireless-N WLAN Mini-Card
Stop
MAC Address | SSID | RSSI | Channel | Vendor | Privacy | Max Rate | Network Type | First Seen | Last Seen | Latitude | Longitude
5C:D9:98:60:EC:40 | gonzaga-norte | -87 | 1 | D-Link Corporation | WEP | 54 | Infrastructure | 8:16:01 | 8:23:19 | 0,000000 | 0,000000
00:26:5A:83:62:02 | Rectorado | -90 | 6 | D-Link Corporation | WEP | 54 | Infrastructure | 8:17:50 | 8:18:59 | 0,000000 | 0,000000
00:15:6D:68:43:E2 | PUNTONET PUENGASI2 | -88 | 9 | Ubiquiti Networks Inc. | None | 11 | Infrastructure | 8:18:27 | 8:19:54 | 0,000000 | 0,000000
1C:AF:F7:4A:89:86 | jym-hh | -86 | 3 | D-LINK INTERNATI... | RSNA-CCMP | 150 (N) | Infrastructure | 8:19:08 | 8:21:11 | 0,000000 | 0,000000
00:18:F8:D7:EC:63 | gonzaga-sur | -84 | 7 | Cisco-Linksys LLC | WEP | 54 | Infrastructure | 8:19:18 | 8:29:18 | 0,000000 | 0,000000
00:1E:58:B8:4B:EB | comunidad | -83 | 1 | D-Link Corporation | WEP | 54 | Infrastructure | 8:19:28 | 8:29:18 | 0,000000 | 0,000000
00:15:6D:55:EC:49 | LaArmenia | -89 | 7 | Ubiquiti Networks Inc. | RSNA-TKIP | 54 | Infrastructure | 8:21:35 | 8:21:46 | 0,000000 | 0,000000
02:0C:42:68:7F:E5 | PUNTONET MIRAVALLE | -88 | 11 | | None | 54 | Infrastructure | 8:21:35 | 8:21:35 | 0,000000 | 0,000000
02:0C:42:68:85:57 | PUNTONET MIRAVALLE2 | -88 | 5 | | None | 54 | Infrastructure | 8:21:48 | 8:21:48 | 0,000000 | 0,000000
00:14:D1:4A:18:FE | The Joker Net | -85 | 1 | TRENDnet | WEP | 54 | Infrastructure | 8:22:11 | 8:24:17 | 0,000000 | 0,000000
News Time Graph 2.4 GHz Channels 5 GHz Channels Filters GPS
Amplitude [dB]
gonzaga-sur
10 / 10 AP(s) GPS: Off
Logging to h.gpx (297,55KB)
inSSIDer 2.0
3.jpg - Paint
ES 8:29

(D)


inSSIDer 2.0
File View Help
Start GPS
Dell Wireless 1510 Wireless-N WLAN Mini-Card
Stop
MAC Address | SSID | RSSI | Channel | Vendor | Privacy | Max Rate | Network Type | First Seen | Last Seen | Latitude | Longitude
5C:D9:98:60:EC:40 gonzaga-norte -72 1 D-Link Corporation WEP 54 Infrastructure 8:16:01 8:34:58 0,000000 0,000000
00:26:5A:83:62:02 Rectorado -90 6 D-Link Corporation WEP 54 Infrastructure 8:17:50 8:18:59 0,000000 0,000000
00:15:6D:68:43:E2 PUNTONET PUENGASI2 -87 9 Ubiquiti Networks Inc. None 11 Infrastructure 8:18:27 8:33:21 0,000000 0,000000
1C:AF:F7:4A:89:B6 jym-hh -82 3 + 7 D-LINK INTERNATI... RSNA-CCMP 150 (N) Infrastructure 8:19:08 8:34:58 0,000000 0,000000
00:18:F8:D7:EC:63 gonzaga-sur -86 7 Cisco-Linksys LLC WEP 54 Infrastructure 8:19:18 8:34:58 0,000000 0,000000
00:1E:58:B8:4B:EB comunidad -86 1 D-Link Corporation WEP 54 Infrastructure 8:19:28 8:34:58 0,000000 0,000000
00:15:6D:55:EC:49 LaArmenia -88 7 Ubiquiti Networks Inc. RSNA-TKIP 54 Infrastructure 8:21:35 8:33:59 0,000000 0,000000
02:0C:42:68:7F:E5 PUNTONET MIRAVALLE -88 11 None 54 Infrastructure 8:21:35 8:21:35 0,000000 0,000000
02:0C:42:68:85:57 PUNTONET MIRAVALLE2 -88 5 None 54 Infrastructure 8:21:48 8:21:48 0,000000 0,000000
00:14:D1:4A:18:FE The Joker Net -85 1 TRENDnet WEP 54 Infrastructure 8:22:11 8:32:47 0,000000 0,000000
00:18:11:4E:63:D7 eduwifi -90 11 D-Link Corporation WPA-TKIP 11 Infrastructure 8:30:01 8:34:56 0,000000 0,000000
02:15:6D:65:BA:AF BS15106SE10 -86 40 None 54 Infrastructure 8:31:22 8:31:49 0,000000 0,000000
02:15:6D:65:BA:AA BS15106SE03 -84 40 None 54 Infrastructure 8:31:24 8:31:24 0,000000 0,000000
News Time Graph 2.4 GHz Channels 5 GHz Channels Filters GPS
Amplitude [dB]
gonzaga-sur
25 / 25 AP(s) GPS: Off Logging to h.gpx (661,26KB)
inSSIDer 2.0 4.jpg - Paint Connect to a network ES 8:34

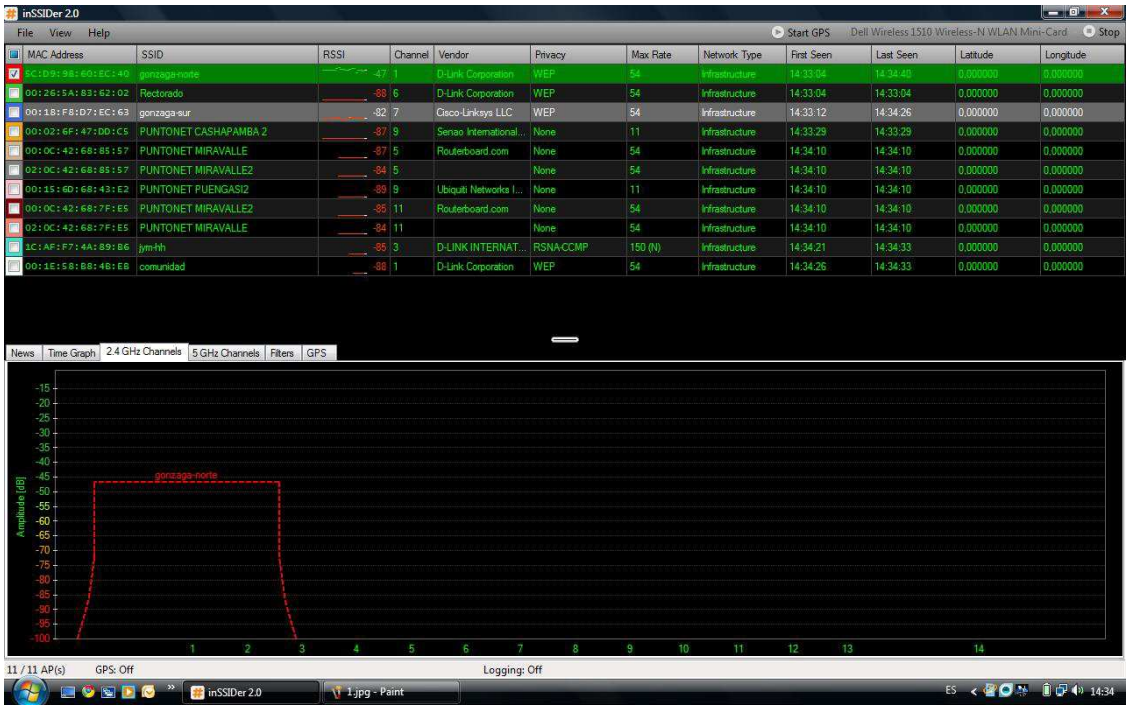
(E)


inSSIDer 2.0
File View Help
Start GPS
Dell Wireless 1510 Wireless-N WLAN Mini-Card
Stop
MAC Address | SSID | RSSI | Channel | Vendor | Privacy | Max Rate | Network Type | First Seen | Last Seen | Latitude | Longitude
5C:D9:98:60:EC:40 gonzaga-norte -56 1 D-Link Corporation WEP 54 Infrastructure 8:16:01 8:36:43 0,000000 0,000000
00:26:5A:83:62:02 Rectorado -90 6 D-Link Corporation WEP 54 Infrastructure 8:17:50 8:18:59 0,000000 0,000000
00:15:6D:68:43:E2 PUNTONET PUENGASI2 -88 9 Ubiquiti Networks Inc. None 11 Infrastructure 8:18:27 8:35:47 0,000000 0,000000
1C:AF:F7:4A:89:B6 jym-hh -86 3 D-LINK INTERNATI... RSNA-CCMP 150 (N) Infrastructure 8:19:08 8:36:18 0,000000 0,000000
00:18:F8:D7:EC:63 gonzaga-sur -88 7 Cisco-Linksys LLC WEP 54 Infrastructure 8:19:18 8:36:20 0,000000 0,000000
00:1E:58:B8:4B:EB comunidad -90 1 D-Link Corporation WEP 54 Infrastructure 8:19:28 8:36:07 0,000000 0,000000
00:15:6D:55:EC:49 LaArmenia -88 7 Ubiquiti Networks Inc. RSNA-TKIP 54 Infrastructure 8:21:35 8:33:59 0,000000 0,000000
02:0C:42:68:7F:E5 PUNTONET MIRAVALLE -88 11 None 54 Infrastructure 8:21:35 8:21:35 0,000000 0,000000
02:0C:42:68:85:57 PUNTONET MIRAVALLE2 -88 5 None 54 Infrastructure 8:21:48 8:21:48 0,000000 0,000000
00:14:D1:4A:18:FE The Joker Net -85 1 TRENDnet WEP 54 Infrastructure 8:22:11 8:32:47 0,000000 0,000000
00:18:11:4E:63:D7 eduwifi -88 11 D-Link Corporation WPA-TKIP 11 Infrastructure 8:30:01 8:36:20 0,000000 0,000000
02:15:6D:65:BA:AF BS15106SE10 -86 40 None 54 Infrastructure 8:31:22 8:31:49 0,000000 0,000000
02:15:6D:65:BA:AA BS15106SE03 -84 40 None 54 Infrastructure 8:31:24 8:31:24 0,000000 0,000000
News Time Graph 2.4 GHz Channels 5 GHz Channels Filters GPS
Amplitude [dB]
27 / 27 AP(s) GPS: Off Logging to h.gpx (756,67KB)
inSSIDer 2.0 5.jpg - Paint Connect to a network ES 8:36

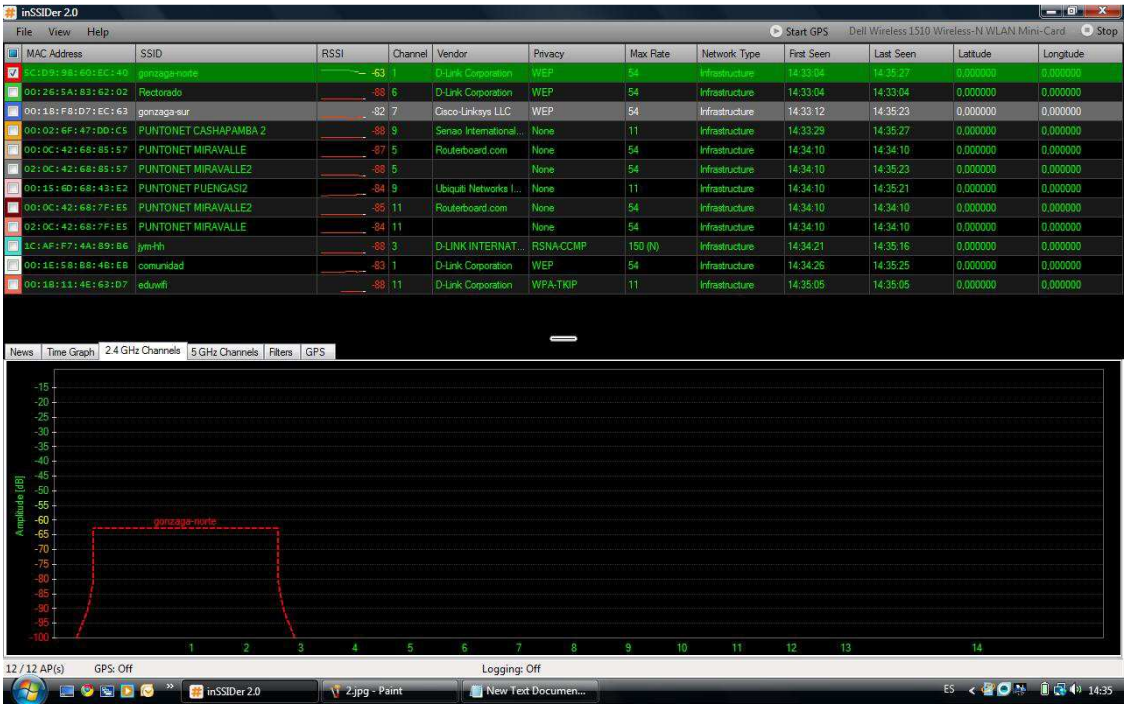
(F)


inSSIDer 2.0
File View Help
Start GPS
Dell Wireless 1510 Wireless-N WLAN Mini-Card
Stop
MAC Address | SSID | RSSI | Channel | Vendor | Privacy | Max Rate | Network Type | First Seen | Last Seen | Latitude | Longitude
5C:D9:98:60:EC:40 | gonzaga-norte | -46 | 1 | D-Link Corporation | WEP | 54 | Infrastructure | 15:40:56 | 15:41:29 | 0,000000 | 0,000000
00:18:F8:D7:EC:63 | gonzaga-sur | -86 | 7 | Cisco-Linksys LLC | WEP | 54 | Infrastructure | 15:40:58 | 15:41:22 | 0,000000 | 0,000000
00:0C:42:68:7F:E5 | PUNTONET MIRAVALLE2 | -87 | 11 | Routerboard.com | None | 54 | Infrastructure | 15:41:10 | 15:41:10 | 0,000000 | 0,000000
00:15:6D:68:43:E2 | PUNTONET PUENGASI2 | -88 | 9 | Ubiquiti Networks I... | None | 11 | Infrastructure | 15:41:14 | 15:41:14 | 0,000000 | 0,000000
News | Time Graph | 2.4 GHz Channels | 5 GHz Channels | Filters | GPS
Amplitude [dB]
gonzaga-norte
4 / 4 AP(s)
GPS: Off
Logging: Off
New Text Documen...
inSSIDer 2.0
ES
15:41

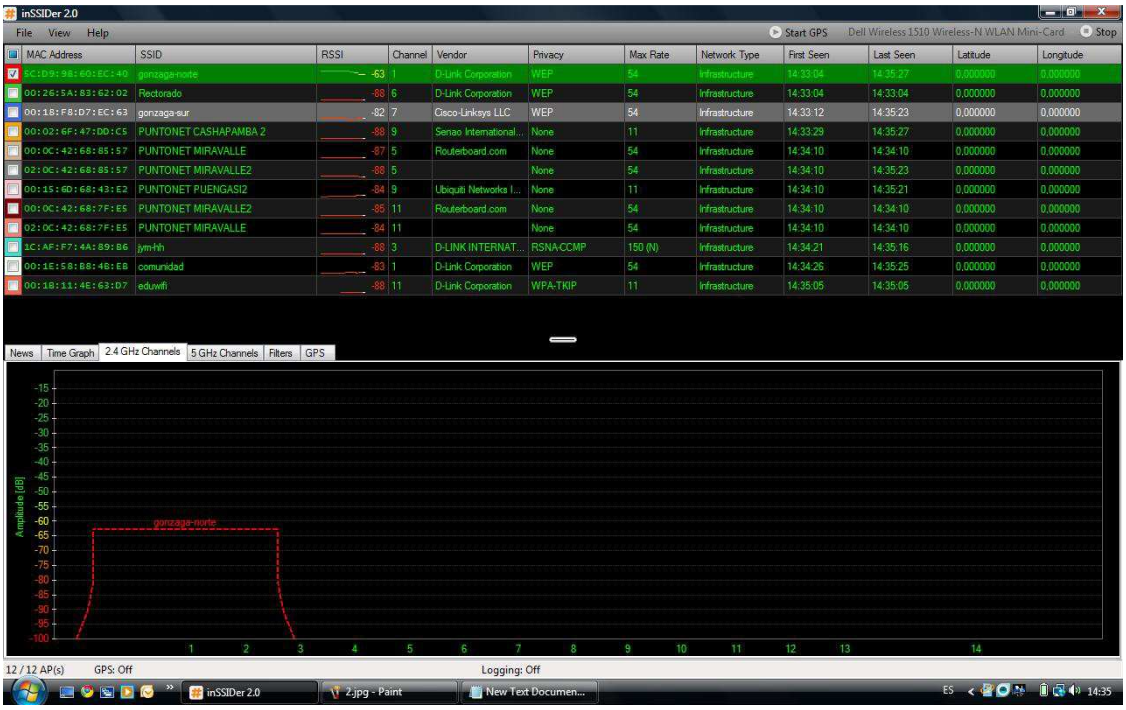
(G)


inSSIDer 2.0
File View Help
Start GPS
Dell Wireless 1510 Wireless-N WLAN Mini-Card
Stop
MAC Address | SSID | RSSI | Channel | Vendor | Privacy | Max Rate | Network Type | First Seen | Last Seen | Latitude | Longitude
5C:D9:98:60:EC:40 | gonzaga-norte | -47 | 1 | D-Link Corporation | WEP | 54 | Infrastructure | 14:33:04 | 14:34:40 | 0,000000 | 0,000000
00:26:5A:83:62:02 | Rectorado | -88 | 6 | D-Link Corporation | WEP | 54 | Infrastructure | 14:33:04 | 14:33:04 | 0,000000 | 0,000000
00:18:F8:D7:EC:63 | gonzaga-sur | -82 | 7 | Cisco-Linksys LLC | WEP | 54 | Infrastructure | 14:33:12 | 14:34:26 | 0,000000 | 0,000000
00:02:6F:47:DD:C5 | PUNTONET CASHAPAMBA 2 | -87 | 9 | Senao International... | None | 11 | Infrastructure | 14:33:29 | 14:33:29 | 0,000000 | 0,000000
00:0C:42:68:85:57 | PUNTONET MIRAVALLE | -87 | 5 | Routerboard.com | None | 54 | Infrastructure | 14:34:10 | 14:34:10 | 0,000000 | 0,000000
02:0C:42:68:85:57 | PUNTONET MIRAVALLE2 | -84 | 5 | | None | 54 | Infrastructure | 14:34:10 | 14:34:10 | 0,000000 | 0,000000
00:15:6D:68:43:E2 | PUNTONET PUENGASI2 | -89 | 9 | Ubiquiti Networks I... | None | 11 | Infrastructure | 14:34:10 | 14:34:10 | 0,000000 | 0,000000
00:0C:42:68:7F:E5 | PUNTONET MIRAVALLE2 | -95 | 11 | Routerboard.com | None | 54 | Infrastructure | 14:34:10 | 14:34:10 | 0,000000 | 0,000000
02:0C:42:68:7F:E5 | PUNTONET MIRAVALLE | -84 | 11 | | None | 54 | Infrastructure | 14:34:10 | 14:34:10 | 0,000000 | 0,000000
1C:AF:F7:4A:B9:B6 | jym-hh | -85 | 3 | D-LINK INTERNAT... | RSNA-CCMP | 150 (N) | Infrastructure | 14:34:21 | 14:34:33 | 0,000000 | 0,000000
00:1E:58:B8:4B:E8 | comunidad | -88 | 1 | D-Link Corporation | WEP | 54 | Infrastructure | 14:34:26 | 14:34:33 | 0,000000 | 0,000000
News | Time Graph | 2.4 GHz Channels | 5 GHz Channels | Filters | GPS
Amplitude [dB]
gonzaga-norte
11 / 11 AP(s)
GPS: Off
Logging: Off
inSSIDer 2.0
1.jpg - Paint
ES
14:34

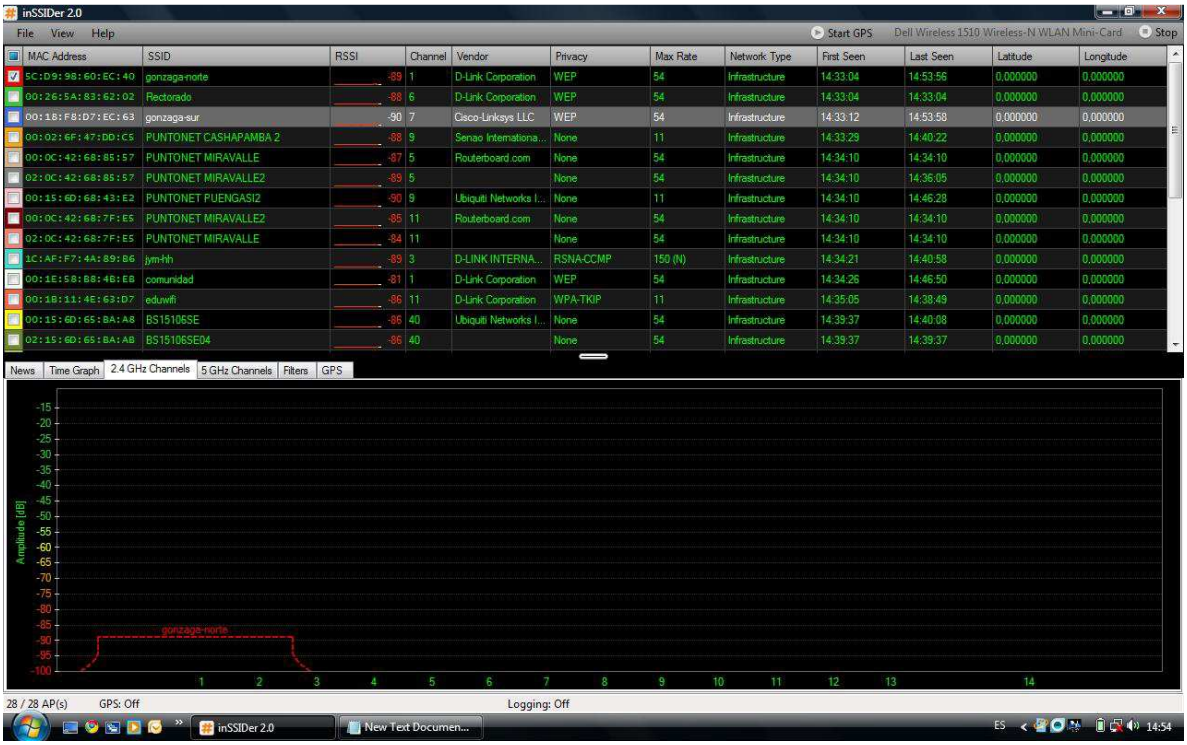
(H)


inSSIDer 2.0
File View Help
Start GPS
Dell Wireless 1510 Wireless-N WLAN Mini-Card
Stop
MAC Address | SSID | RSSI | Channel | Vendor | Privacy | Max Rate | Network Type | First Seen | Last Seen | Latitude | Longitude
5C:D9:98:60:EC:40 gonzaga-norte -63 1 D-Link Corporation WEP 54 Infrastructure 14:33:04 14:35:27 0,000000 0,000000
00:26:5A:83:62:02 Rectorado -88 6 D-Link Corporation WEP 54 Infrastructure 14:33:04 14:33:04 0,000000 0,000000
00:1B:F8:D7:EC:63 gonzaga-sur -82 7 Cisco-Linksys LLC WEP 54 Infrastructure 14:33:12 14:35:23 0,000000 0,000000
00:02:6F:47:DD:C5 PUNTONET CASHAPAMBA 2 -88 9 Senao International... None 11 Infrastructure 14:33:29 14:35:27 0,000000 0,000000
00:0C:42:68:85:57 PUNTONET MIRAVALLE -87 5 Routerboard.com None 54 Infrastructure 14:34:10 14:34:10 0,000000 0,000000
02:0C:42:68:85:57 PUNTONET MIRAVALLE2 -88 5 None 54 Infrastructure 14:34:10 14:35:23 0,000000 0,000000
00:15:6D:68:43:E2 PUNTONET PUENGASI2 -84 9 Ubiquiti Networks I... None 11 Infrastructure 14:34:10 14:35:21 0,000000 0,000000
00:0C:42:68:7F:E5 PUNTONET MIRAVALLE2 -85 11 Routerboard.com None 54 Infrastructure 14:34:10 14:34:10 0,000000 0,000000
02:0C:42:68:7F:E5 PUNTONET MIRAVALLE -84 11 None 54 Infrastructure 14:34:10 14:34:10 0,000000 0,000000
1C:AF:F7:4A:89:B6 jym-hh -88 3 D-LINK INTERNAT... RSNA-CCMP 150 (N) Infrastructure 14:34:21 14:35:16 0,000000 0,000000
00:1E:58:B8:4B:EB comunidad -83 1 D-Link Corporation WEP 54 Infrastructure 14:34:26 14:35:25 0,000000 0,000000
00:1B:11:4E:63:D7 eduwifi -88 11 D-Link Corporation WPA-TKIP 11 Infrastructure 14:35:05 14:35:05 0,000000 0,000000
News Time Graph 2.4 GHz Channels 5 GHz Channels Filters GPS
Amplitude [dB]
gonzaga-norte
12 / 12 AP(s) GPS: Off Logging: Off
inSSIDer 2.0
2.jpg - Paint
New Text Documen...
ES 14:35

(I)


inSSIDer 2.0
File View Help
Start GPS
Dell Wireless 1510 Wireless-N WLAN Mini-Card
Stop
MAC Address | SSID | RSSI | Channel | Vendor | Privacy | Max Rate | Network Type | First Seen | Last Seen | Latitude | Longitude
5C:D9:98:60:EC:40 gonzaga-norte -63 1 D-Link Corporation WEP 54 Infrastructure 14:33:04 14:35:27 0,000000 0,000000
00:26:5A:83:62:02 Rectorado -88 6 D-Link Corporation WEP 54 Infrastructure 14:33:04 14:33:04 0,000000 0,000000
00:1B:F8:D7:EC:63 gonzaga-sur -82 7 Cisco-Linksys LLC WEP 54 Infrastructure 14:33:12 14:35:23 0,000000 0,000000
00:02:6F:47:DD:C5 PUNTONET CASHAPAMBA 2 -88 9 Senao International... None 11 Infrastructure 14:33:29 14:35:27 0,000000 0,000000
00:0C:42:68:85:57 PUNTONET MIRAVALLE -87 5 Routerboard.com None 54 Infrastructure 14:34:10 14:34:10 0,000000 0,000000
02:0C:42:68:85:57 PUNTONET MIRAVALLE2 -88 5 None 54 Infrastructure 14:34:10 14:35:23 0,000000 0,000000
00:15:6D:68:43:E2 PUNTONET PUENGASI2 -84 9 Ubiquiti Networks I... None 11 Infrastructure 14:34:10 14:35:21 0,000000 0,000000
00:0C:42:68:7F:E5 PUNTONET MIRAVALLE2 -85 11 Routerboard.com None 54 Infrastructure 14:34:10 14:34:10 0,000000 0,000000
02:0C:42:68:7F:E5 PUNTONET MIRAVALLE -84 11 None 54 Infrastructure 14:34:10 14:34:10 0,000000 0,000000
1C:AF:F7:4A:89:B6 jym-hh -88 3 D-LINK INTERNAT... RSNA-CCMP 150 (N) Infrastructure 14:34:21 14:35:16 0,000000 0,000000
00:1E:58:B8:4B:EB comunidad -83 1 D-Link Corporation WEP 54 Infrastructure 14:34:26 14:35:25 0,000000 0,000000
00:1B:11:4E:63:D7 eduwifi -88 11 D-Link Corporation WPA-TKIP 11 Infrastructure 14:35:05 14:35:05 0,000000 0,000000
News Time Graph 2.4 GHz Channels 5 GHz Channels Filters GPS
Amplitude [dB]
gonzaga-norte
12 / 12 AP(s) GPS: Off Logging: Off
inSSIDer 2.0
2.jpg - Paint
New Text Documen...
ES 14:35

(J)



(K)

Figura 2.7: Análisis de datos con software Site Survey

(A) Intensidad de señal inalámbrica de red Gonzaga-Sur a 4 metros del Access Point.

(B) Intensidad de señal inalámbrica de red Gonzaga-Sur a 20 metros del Access Point.

(C) Intensidad de señal inalámbrica de red Gonzaga-Sur a 35 metros del Access Point.

(D) Intensidad de señal inalámbrica de red Gonzaga-Sur a 45 metros del Access Point.

(E) Intensidad de señal inalámbrica de red Gonzaga-Sur a 56 metros del Access Point.

(F) Intensidad de señal inalámbrica de red Gonzaga-Sur a 68 metros del Access Point.

(G) Intensidad de señal inalámbrica de red Gonzaga-Norte a 3 metros del Access Point.

(H) Intensidad de señal inalámbrica de red Gonzaga-Norte a 15 metros del Access Point.

(I) Intensidad de señal inalámbrica de red Gonzaga-Norte a 28 metros del Access Point.

(J) Intensidad de señal inalámbrica de red Gonzaga-Norte a 58 metros del Access Point.

(K) Intensidad de señal inalámbrica de red Gonzaga-Norte a 90 metros del Access Point.

Fuente: Software SiteSurvey inSSIDer 2.0

Interpretando estos gráficos se tiene como referencia que:

- Los routers inalámbricos marca Linksys modelos WRT54GL (Gonzaga-Sur) y WRT160NL, proveen de intensidad de señal a una distancia promedio de 101 metros en línea de vista. Pero a una distancia de 96,85 metros del router inalámbrico, se pierde en un 90% la conectividad hacia la red local e internet. Dando así un distancia total de cobertura de 95 metros en línea de vista.

- Router inalámbrico marca D-Link DIR 615(Gonzaga-Norte) provee de intensidad de señal a una distancia de 95,40 metros en línea de vista. Pero a una distancia de 91 metros del router inalámbrico, se pierde en un 90% la conectividad hacia la red local e internet. Dando así un distancia total de cobertura de 90 metros en línea de vista.

La implementación del Portal Cautivo para las instalaciones del Colegio San Luis Gonzaga deberá cubrir como punto central la Biblioteca P. Gonzalo Romero S.J. (Identificado en el Grafico 14), ubicado en el sector sur del Colegio. Por lo que se utilizará el router inalámbrico Linksys WRT160NL inactivo, ya que con el alcance máximo de la señal inalámbrica obtenido en base a la utilización de software site survey, y con la referencia del router inalámbrico Linksys WRT54GL instalado a un costado de la Biblioteca, la señal cubrirá con mucho lo necesitado para este fin.

CAPÍTULO 3

DESCRIPCIÓN DE HARDWARE Y SOFTWARE A UTILIZAR PARA LA IMPLEMENTACIÓN DEL PORTAL CAUTIVO

En el presente capítulo se describirá los recursos de hardware y de software que serán utilizados para la implementación del portal cautivo en todas sus dimensiones.

La descripción comenzará por el hardware en el cual se sustentará todo el portal cautivo, siguiendo por describir, el software que se instalará y configurará para la puesta en marcha del Portal Cautivo como sistema adicional de seguridad para los estudiantes del Colegio San Luis Gonzaga que se conectarán a la red inalámbrica.

3.1 DESCRIPCIÓN DE HARDWARE

En cuanto a la descripción del hardware que se utilizará para la implementación del portal cautivo, se tiene que, son dos los componentes indispensables sobre los cuales se manejará todo el proceso de autenticación y autorización del servicio de conectividad en la red inalámbrica.

DISPOSITIVO	DESCRIPCIÓN
Servidor	Computador de Escritorio
Router Inalámbrico	Linksys WR160NL

Tabla 3.1: Dispositivos hardware a utilizar para la implementación de portal cautivo.

Fuente: Autor de la Tesis.

Antes de poder instalar el software necesario de sistema operativo, servicio de portal cautivo, servicio de autenticación, almacenamiento de usuarios y configuración de seguridad, se deberá definir requisitos mínimos de hardware sobre los cuales se instalarán los servicios ya mencionados, con su respectivo software.

El hardware necesario está integrado en un computador de escritorio que realizará la función de servidor, el mencionado computador contará con las siguientes características:

HARDWARE	
Procesador:	Dual Core 1.6 GHz
Disco Duro:	160 GB
Memoria RAM:	2GB
Interfaces de Red:	2 interfaces de red Ethernet

Tabla 3.2: Características de Hardware Computador con función de Servidor.

Fuente: Autor de la Tesis.

Las características mencionadas en la Tabla 3.2, pretenden abarcar los requisitos mínimos recomendados de hardware para la instalación de los distintos tipos de software, los cuales brindarán los servicios necesarios para que un usuario pueda utilizar del portal cautivo. En la siguiente tabla se muestra los tipos de software a instalar:

SOFTWARE	
Debian 6	Sistema operatvo
Freeradius	Software para autenticación de usuarios
MySQL	Gestor de Base de Datos
Chillispot	Software interfaz para acceder al portal cautivo.

Tabla 3.3: Software a instalar dentro del computador (Servidor).

Fuente: Autor de la Tesis.

REQUISITOS PARA INSTALACIÓN DE SISTEMA OPERATIVO (DEBIAN 6 GNU/LINUX)

- **Procesador:** Pentium 4, 1GHz
- **Disco Duro:**1GB (Sin entorno gráfico), 5 GB (Con entorno gráfico)
- **Memoria RAM**: 256 MB (Sin entorno gráfico), 512 MB (Con entorno gráfico)[20]

REQUISITOS PARA INSTALACIÓN DEL SERVIDOR RADIUS (FREERADIUS)

- **Procesador:** Pentium 4, 1GHz
- **Disco Duro:**80GB
- **Memoria RAM:** 256 MB[21]

20 Esta información es obtenida desde el portal oficial Debian, en el artículo "Guía de instalación de Debian GNU/Linux", http://www.chillispot.info

21Estos requerimientos son tomados en base a las recomendaciones de hardware que se da para instalar el sistema operativo, ya que su administración no requiere de un potencial mayor en cuanto a hardware.

REQUISITOS PARA INSTALACIÓN SERVIDOR BASE DE DATOS (MYSQL)

- **Procesador:** Pentium 4, 1GHz
- **Disco Duro:** 500 MB
- **Memoria RAM:** 512 MB[22]

REQUISITOS PARA INSTALACIÓN DE PORTAL CAUTIVO (CHILLISPOT)

Para la instalación de Chillispot como base del portal cautivo, no se tiene una referencia con requerimientos mínimos de hardware, por lo que, por ser un software de licencia tipo GNU, podrá ser instalado en cualquier computador de escritorio o servidor actualizado.

Con la identificación del hardware mínimo necesario para todos los servicios que ofrecerá la implementación del portal cautivo se tiene un valor de sumatoria con el cual se referencia al computador que será utilizado como servidor. Dicha información se presenta en la siguiente tabla:

HARDWARE	SERVICIO				
	Freeradius	**MySQL**	**Debian**	**Chillispot**	**Sumatoria**
Procesador	Pentium 4	Pentium 4	Pentium 4	----------	----------
Disco Duro	80 GB	500 MB (0,488 GB)	5 GB	----------	85,488 GB
Memoria RAM	256 MB	512 MB	512 MB	----------	1280 MB (1,25 GB)

Tabla 3.4: Sumatoria de valores hardware para dimensionar CPU Servidor.

Fuente: Autor de la Tesis.

22 [Arakhne]

Conocidos ya, estos valores de sumatoria total, se puede reflejar una capacidad superior en las características de hardware del computador que realizará la función de servidor (Tabla 3.2) en comparación con los valores obtenidos en la Tabla 3.4, para la implementación y correcto funcionamiento del portal cautivo.

ROUTER INALÁMBRICO LINKSYS WRT160NL

El router inalámbrico escogido sobre el cual se montará y por consiguiente difundirá el portal cautivo es un Linksys WRT160NL, seleccionado por su agilidad de conectividad, ofreciendo las siguientes características:

- Utiliza un firmware con licencia tipo GNU con posibilidad de un upgrade de firmware.
- Trabaja con el estándar 802.11 b, 802.11 g y 802.11 n.
- Soporta servicio DHCP (Asignación de IP's dinámica)

Teniendo en cuenta las características mencionadas, se escogió este tipo de router inalámbrico por la facilidad que genera la configuración directa al portal cautivo con Chillispot y al servidor Freeradius que permite la autenticación de usuarios.

3.2 DESCRIPCIÓN DE SOFTWARE

Una vez definido el hardware necesario para el presente proyecto, se debe identificar el software que será base imprescindible en el objetivo de montar un sistema adicional de seguridad de red, portal cautivo.

Antes de la descripción del software, se debe tener en cuenta la relación que van a tener entre cada uno de los programas a mencionar.

Se instalará primero un sistema operativo que cumpla con ser una distribución libre de Linux que, por su robustez, soporte a cada uno de los programas que se

instalarán sobre él. Se instalará además el software que permitirá la autenticación y autorización de los usuarios para su posterior ingreso a la red inalámbrica, se instalará también una base de datos, encargada de garantizar el resguardo de los nombres de usuario y contraseñas que serán aportados por cada uno de los individuos que hagan uso del portal cautivo, esta seguridad e integridad de información será otorgada por un software en particular el cual creará una encriptación para mantener la seguridad en la transmisión de paquetes de datos bajo buen recaudo y protección, y por último se instalará el software que permitirá establecer la interfaz mediante la cual los usuarios podrán conectarse a la red del Colegio San Luis Gonzaga.

Los programas que se describirán a continuación son:

SOFTWARE	SERVICIO
Debian 6 GNU/Linux	Sistema Operativo.
Freeradius	Software de Autenticación, Autorización y Contabilidad de usuarios.
OpenSSL	Herramientas de administración para seguridad en el transporte de paquetes de información.
MySQL	Software Gestor de Base de Datos.
PhpMyAdmin	Software que administra Bases de Datos a través de entorno web.
Chillispot	Software interfaz para acceder al portal cautivo.

Tabla 3.5: Software a utilizar para la implementación de portal cautivo.

Fuente: Autor de la Tesis.

3.2.1 DEBIAN 6 GNU/LINUX

Distribución del sistema operativo LINUX y conocida como la versión más estable entre todas. En esta versión el núcleo de Linux está completamente libre, ya que los archivos problemáticos de firmware se han dividido en paquetes separados y se han movido fuera del archivo principal de Debian al área no libre (non-free) del archivo, la cual no está activada de manera predeterminada.

De esta forma, se tiene la posibilidad de utilizar un sistema operativo más libre. Los archivos de firmware pueden cargarse durante la instalación a través del instalador si se quiere.

Incluye los entornos de escritorio KDE, GNOME, Xfce y LXDE, así como todo tipo de aplicaciones de servidor. Se ejecuta sobre Pc de 32 bits y 64 bits.

Ejecución en paralelo de los programas de arranque y el seguimiento correcto de sus interdependencias, por lo que Debian arranca mucho más rápido.

Incluye más de 29000 paquetes de programas listos para utilizar entre los cuales están los servidores Apache 2.2.16 y MySQL 5.1.49.

Se utiliza en el presente proyecto de tesis, por su robustez de servicio, por su gran aplicabilidad como servidor múltiple, su disponibilidad continua y adaptación a las necesidades de los usuarios por ser un sistema operativo con licencia abierta.

3.2.2 FREERADIUS

Freeradius es un proyecto iniciado en 1999 por Alan DeKok y Miquel van Smoorenburg.

Es una alternativa libre hacia otros servidores RADIUS, siendo uno de los más completos y versátiles gracias a la variedad de módulos que le componen.

Puede operar tanto en sistemas con recursos limitados así como sistemas atendiendo millones de usuarios. Freeradius permite actualmente una mayor colaboración de la comunidad y que pudiera cubrir las necesidades que otros servidores RADIUS no podían. Freeradius incluye soporte para LDAP, SQL y otras bases de datos, así como EAP, EAP-TTLS y PEAP. Incluye también soporte para todos los protocolos comunes de autenticación y bases de datos.

3.2.3 MYSQL

Software que proporciona un sistema de gestión de base de datos SQL[23] muy rápido, eficaz y robusto. MySQL puede ser incluido en sistemas y en entornos de producción y utilización a nivel crítico.

Entre las principales ventajas que MySQL presenta están:

- MySQL admite gran cantidad de idiomas y caracteres especiales en los datos almacenados.

- MySQL ofrece mayor seguridad de datos ya que todas sus contraseñas están cifradas cuando se conecta al servidor

[23] **SQL** (Structured Query Language - Lenguaje de Consultas Estructurado) Es el lenguaje estandarizado más común de acceso a bases de datos que explota la flexibilidad y potencia de los sistemas relacionales permitiendo gran variedad de operaciones sobre las bases de datos.

- MySQL permite mayor índice de escalabilidad y almacenamiento de datos, llegando a almacenar alrededor de 60.000 tablas en una sola base de datos y con más de 5 trillones de registros.

- MySQL provee de una excelente conectividad tanto en sistemas Windows como Unix, ya que utiliza varios tipos de interfaces de conexión.

3.2.4 PHPMYADMIN

PhpMyAdmin es un software diseñado en lenguaje PHP [24] el cual permite administrar y gestionar bases de datos a través de un entorno web. PhpMyAdmin trabaja especialmente con MySQL y consiente la creación y eliminación de nuevas bases de datos, alteración de tablas e ingreso y modificación de registros de datos. PhpMyAdmin provee de reportes de datos en varios formatos imprimibles o exportables a archivos digitales. Es un software bajo licencia GPL, por lo que se sigue con la línea de instalación de software libre y sin restricción de licencias.

3.2.5 CHILLISPOT

Chillispot es un software que proporciona un portal cautivo de código abierto que permite el acceso de usuarios a una red inalámbrica. La autenticación es procesada mediante un protocolo AAA (Autenticación, Autorización, Contabilidad) manejado por un servidor Radius. Chillispot garantiza que solo naveguen por internet usuarios autorizados y registrados.

[24] **PHP** (Hypertext Pre-Processor) Lenguaje de programación creado para diseñar páginas web dinámicas o implementar aplicaciones con interfaz gráficas.

El sistema de autenticación Chillispot consta de dos partes principales, una es el demonio Chillispot que se encarga de gestionar los clientes de la subred y pedirles autenticación y la otra consta del servidor Radius utilizando el software Freeradius que es quien realiza la autenticación en este caso con el servidor LDAP[25].

Se escoge este software en particular, por su amplia referencia sobre su utilización con el sistema operativo Debian 6. Además de que también es un software con un tipo de licencia libre, siendo fácilmente utilizable sobre cualquier dispositivo que trabaje con distribuciones de Linux.

En el presente capítulo se define que, por la utilización de software de operación y distribución libre, el beneficio de la implementación del portal cautivo es mucho mayor, ya que no se tendrá inconvenientes de licencias o bloqueos al querer utilizar un determinado software en conjunto con otro, además de prestar todo el soporte y robustez en cada uno de los servicios a aplicar.

Este beneficio se ve reflejado en la posibilidad de la reconfiguración de toda la solución del portal cautivo, según sea el caso necesario, y por la posibilidad de instalar y configurar todos los recursos de software sobre un computador que no exija características demasiado altas en cuanto a hardware.

[25] **LDAP** (Lightweight Directory Access Protocol - Protocolo Ligero de Acceso a Directorios) que hace referencia a un protocolo a nivel de aplicación el cual permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red.

CAPÍTULO 4

DISEÑO DE LA SOLUCIÓN A IMPLEMENTARSE EN LA CONFIGURACIÓN DEL PORTAL CAUTIVO Y DEL SERVIDOR RADIUS.

En el presente capítulo, se procederá a diseñar la solución con la cual se contará para poder implementar el portal cautivo. La mencionada solución consiste en la instalación y consiguiente configuración de todas las herramientas de software y hardware que trabajaran en conjunto para poder reflejar un método confiable de seguridad y de restricción de acceso a usuarios, los cuales requieran de conectividad a través la red inalámbrica.

El portal cautivo, contará con tres elementos fundamentales: los clientes o usuarios, el punto de acceso inalámbrico y el servidor de autenticación y autorización.

La interacción positiva de estos tres elementos hará que se pueda justificar la implementación del portal cautivo y hacer útil todo el diseño de la solución en cuanto a la seguridad de acceso para los usuarios de la red inalámbrica.

Para iniciar con la mencionada solución, se comenzará por describir la instalación de cada uno de los programas informáticos a utilizar:

4.1 INSTALACIÓN DE SISTEMA OPERATIVO (DEBIAN 6)

- Como primer paso, se debe bootear el computador, que cumplirá la función de servidor, desde el periférico de lectura óptica (DVD-ROM).
- Se escogerá que tipo de entorno se va a utilizar para instalar el sistema operativo Debían 6, las opciones más comunes a utilizar son mediante una

instalación gráfica (usuarios con conocimiento medio) o una instalación mediante consola (usuarios expertos).

Figura 4.1: Escoger tipo de entorno para instalación de Debian 6.

Fuente: Autor de la Tesis. Debian 6

- Siguiendo con la instalación se deberá completar información básica de idioma, ubicación, tipo de teclado e identificación de máquina (nombre).

- Se configurará la detección de la red de manera automática o de tipo manual. Es importante aclarar que se deberá tener conexión a internet para concluir satisfactoriamente con la instalación de Debian 6.

- Se establecerá la contraseña de superusuario ROOT. La contraseña a configurar deberá tener un gran nivel de seguridad, es decir, utilizar letras mayúsculas y minúsculas e incluso utilizar caracteres numéricos o especiales, con esto se asegura que el superusuario ROOT no sea invadido por ningún usuario no autorizado. El superusuario tiene permiso para configurar todos los servicios del sistema operativo.

Figura 4.2: Configuración de clave para superusuario ROOT.

Fuente: Autor de la Tesis. Debian 6

- Se creará una cuenta de usuario con la que se va a ingresar al equipo para su respectiva administración.

- Se elegirá el espacio físico (disco duro) en el cual se instalará el sistema operativo, este espacio contará con sus respectivas particiones y se deberá escoger una que cuente con espacio libre.

- Se escogerá los programas y paquetes que van a ser necesarios en la instalación y ejecución de Debian 6.

- Una vez configurado todos estos puntos, el sistema operativo Debian 6, comenzará a instalarse para su posterior utilización. En el transcurso de la instalación, Debian 6, descargará los paquetes necesarios para todos los servicios que se vayan a utilizar.

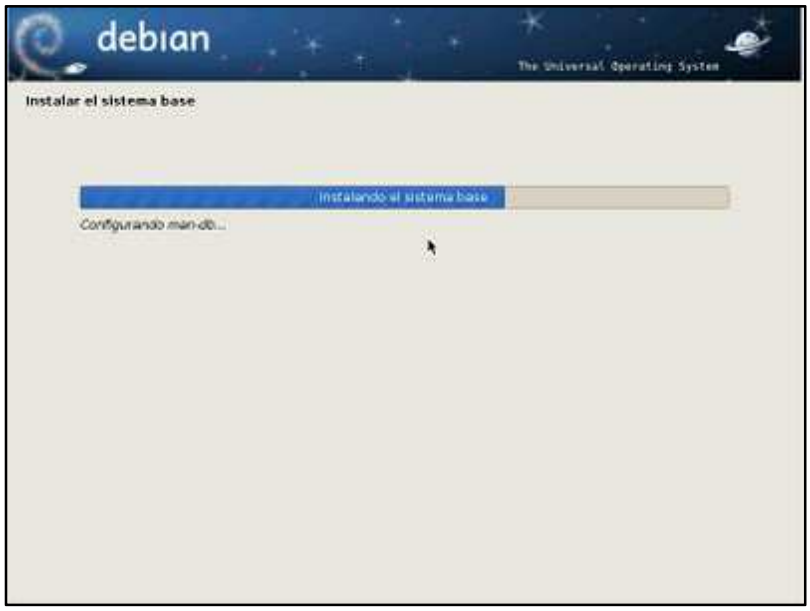


Figura 4.3: Instalación de Sistema Base Debian 6.

Fuente: Autor de la Tesis. Debian 6

- Posterior a la instalación de todo el sistema y sus complementos, se ejecutará el escritorio gráfico del sistema operativo Debian 6.

Figura 4.4: Escritorio gráfico de Debian 6.

Fuente: Autor de la Tesis. Debian 6

Una vez instalado y ejecutado el sistema operativo, se procederá a descargar e instalar cada uno de los programas necesarios.

Para la instalación de los programas y paquetes necesarios para la construcción del Portal Cautivo se debe tener en cuenta que:

- La conexión a internet debe ser permanente para poder descargar e instalar el software.

- Todas las instalaciones se las realizará mediante línea de comandos, por lo se deberá abrir una ventana de Terminal para superusuario ROOT.

Posteriormente se actualiza la lista de paquetes disponibles en los repositorios a utilizar, con lo cual se obtiene la versión más actual de los programas que se instalarán, para este fin se utilizará las siguientes instrucciones:

 # apt-get update (Actualiza los paquetes de los repositorios[26])

 # apt-get upgrade (Instala los paquetes actualizados en los repositorios)

4.2 INSTALACIÓN DE SOFTWARE

Como configuración inicial en el Sistema Operativo se deberá habilitar el soporte TUN/TAP para interfaces virtuales. Este tipo de soporte ofrece transmisión y recepción de paquetes de programas que están dentro del espacio de usuario.
"Puede ser visto como un simple dispositivo Punto a Punto o Ethernet, el cual en vez de recibir paquetes a través de un medio físico, los recibe desde programas del espacio de usuario y en vez de enviarlos por un medio físico los escribe en el espacio de usuario."[27]

[26] **Repositorios**: Un repositorio es un sitio centralizado donde se almacena y mantiene información digital, habitualmente bases de datos o programas/archivos informáticos.

[27] http://linuxeros-faq.blogspot.com/2009/06/tuntap.html, Blog sobre Linux y Software Libre, 26 de julio de 2011

El driver TUN/TAP se utilizará para la transmisión segura de los datos de los usuarios desde Chillispot hacia el servidor Freeradius, por lo que es indispensable que se tenga instalado este componente. Para habilitar este driver se deberá digitar desde una terminal el siguiente comando: *# modconf*

Modconf es una aplicación que permitirá manejar la configuración de controladores de dispositivos. En el caso de no tener instalado esta aplicación se utilizará el siguiente comando para instalarla: *# apt-get install modconf*

Posteriormente aparecerá un recuadro mostrando las categorías de los módulos soportados por el sistema. Se ubicará, la categoría: kernel/drivers/net.

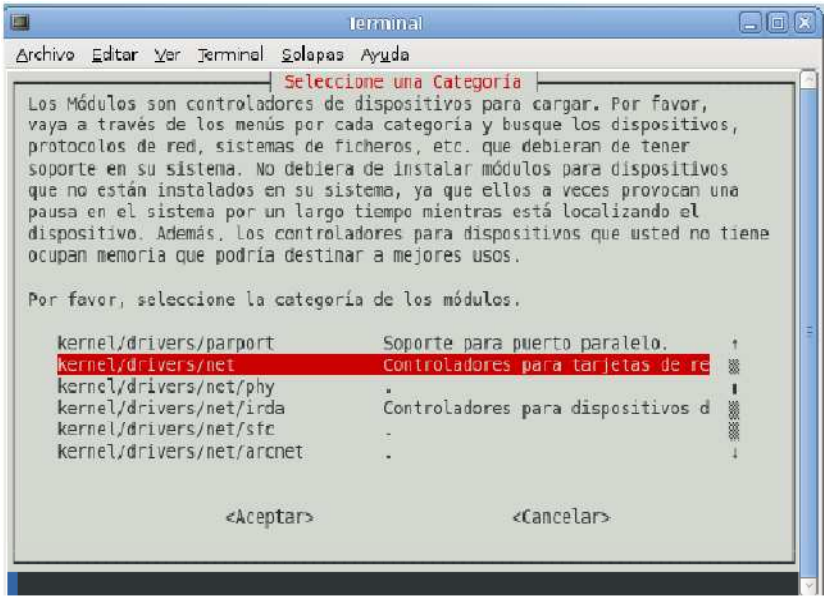


Figura 4.5: Categorías de los módulos soportados por Debian 6.

Fuente: Autor de la Tesis. Debian 6

Dentro de esta categoría se deberá ubicar el módulo “tun – Universal TUN/TAP device driver”. El mencionado módulo deberá mostrar un signo + frente a su descripción, lo cual indica que está instalado y es soportado por el sistema operativo, en el caso de que no se muestre un signo +, se deberá instalar este módulo escogiéndolo y presionando la opción aceptar.

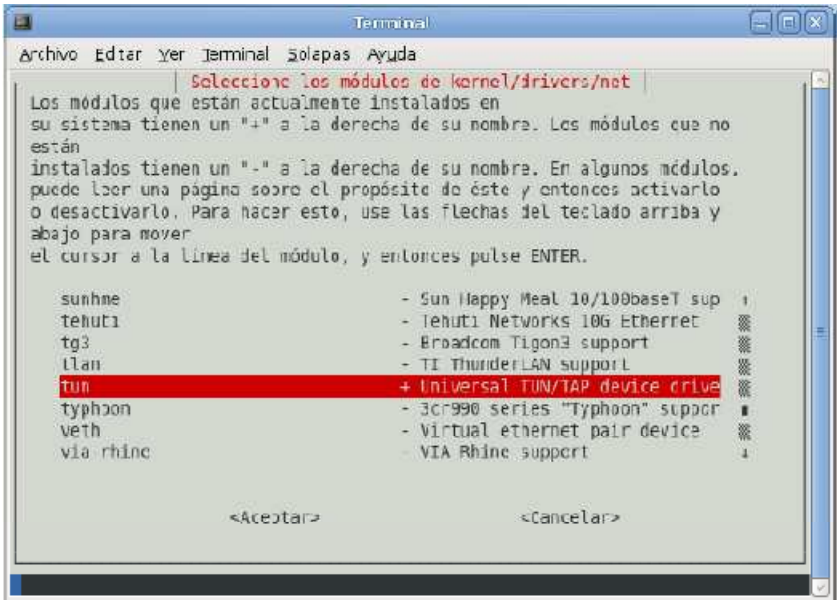


Figura 4.6: Módulo tun soportado por el Debian 6.

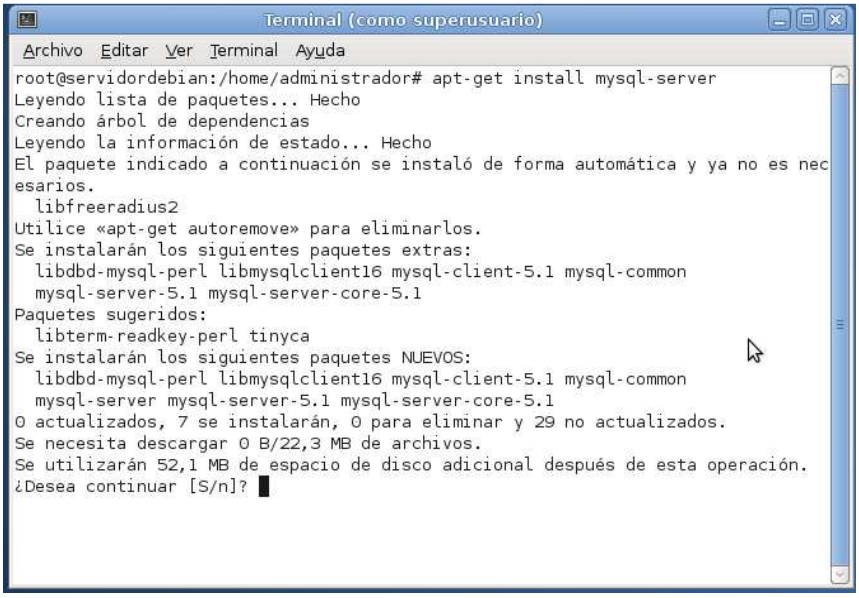
Fuente: Autor de la Tesis. Debian 6

4.2.1 INSTALACIÓN DE BASE DE DATOS MYSQL

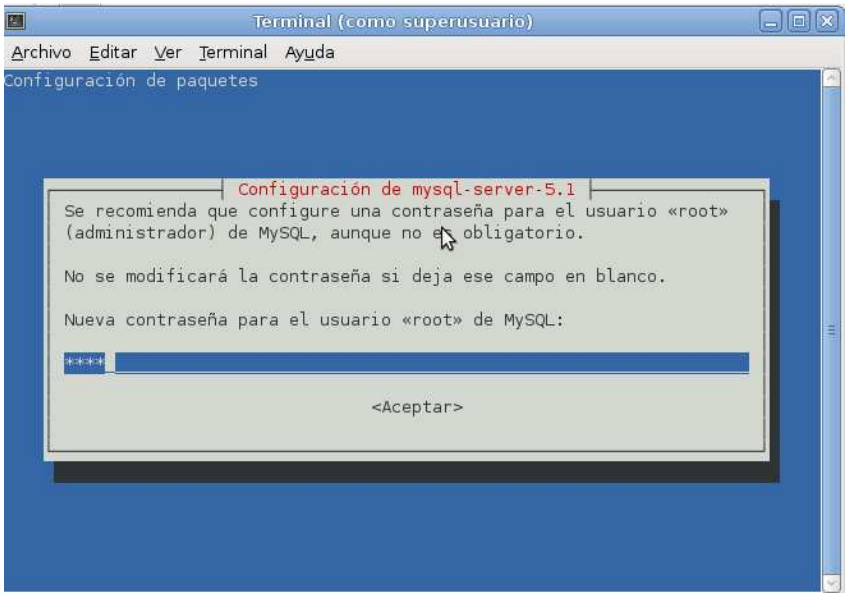
Como primer paquete a instalar se tiene al gestor de base de datos, utilizando MySQL por su descripción y beneficios ya mencionados en el tema de descripción del software en el Capítulo 3.

Se utilizará el siguiente comando:

 # apt-get install mysql-server



(A)



(B)

Figura 4.7: Instalación de MySQL en Debian

(A) Instalación de MySQL en Debian.

(B) Ingreso de contraseña para el usuario ROOT en MySQL.

Fuente: Autor de la Tesis.

4.2.2 INSTALACIÓN DE PHPMYADMIN

Para gestionar la base que trabajará con el servidor Freeradius de forma gráfica, se instalará phpMyAdmin utilizando el siguiente comando: # *apt-get install phpmyadmin*

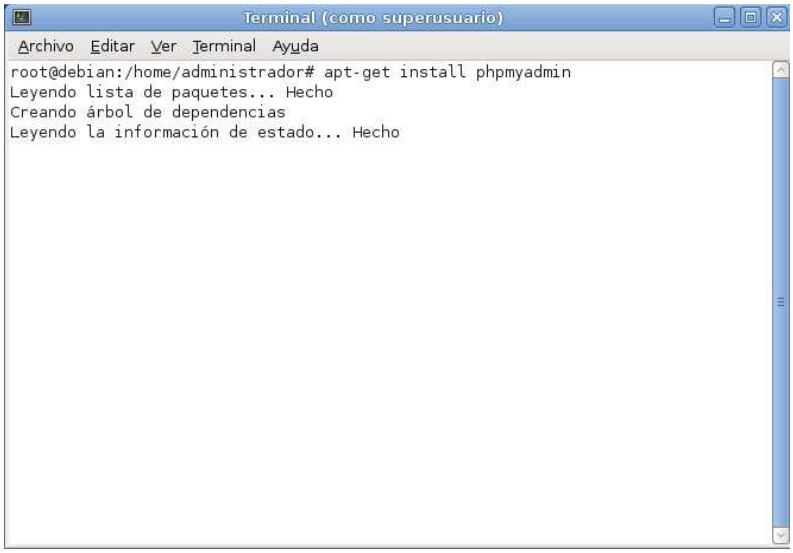


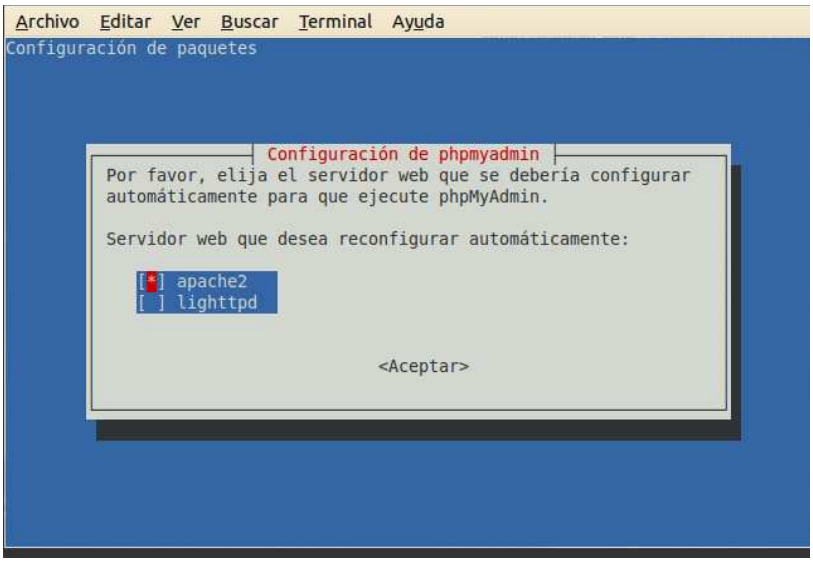
Figura 4.8: Instalación de phpMyAdmin en Debian.

Fuente: Autor de la Tesis.

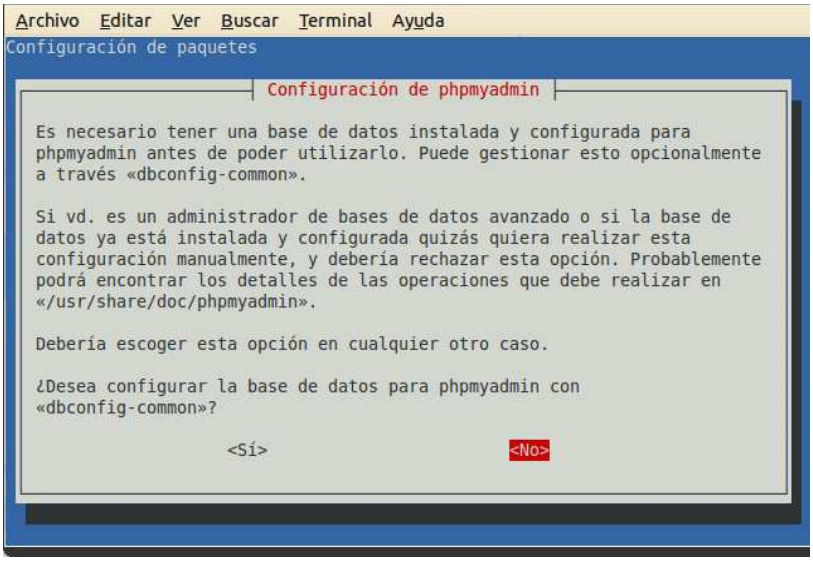
A continuación se debe especificar una clave de acceso para utilizar el entorno web de phpMyAdmin. En este caso la clave a utilizar fue “root” al igual que el nombre de usuario.

Se debe especificar sobre que servidor web trabajará phpMyAdmin, se elegirá la opción “apache2” utilizando la barra espaciadora para marcar la opción escogida.

Para concluir la instalación de phpMyAdmin, se deberá proporcionar la información pertinente para configurar la base de datos propia de phpMyAdmin. Es indispensable realizar este requerimiento y se lo puede hacer mediante la opción dbconfig-common, si este proceso no se realizó no se podrá utilizar el servicio de gestión de datos.



(A)



(B)

Figura 4.9: Instalación de Apache.

(A) Seleccionar el servidor web apache2 sobre el que trabajará phpMyAdmin.

(B) Elegir la opción Sí para la configuración de la base de datos de phpMyAdmin.

Fuente: Autor de la Tesis.

4.2.3 INSTALACIÓN DE FREERADIUS

Para la descarga e instalación de Freeradius se tiene el siguiente comando:

 # apt-get install freeradius freeradius-mysql freeradius-utils

En este comando se incluyen los módulos de Freeradius con MySQL y las herramientas de conexión y utilización de Freeradius.

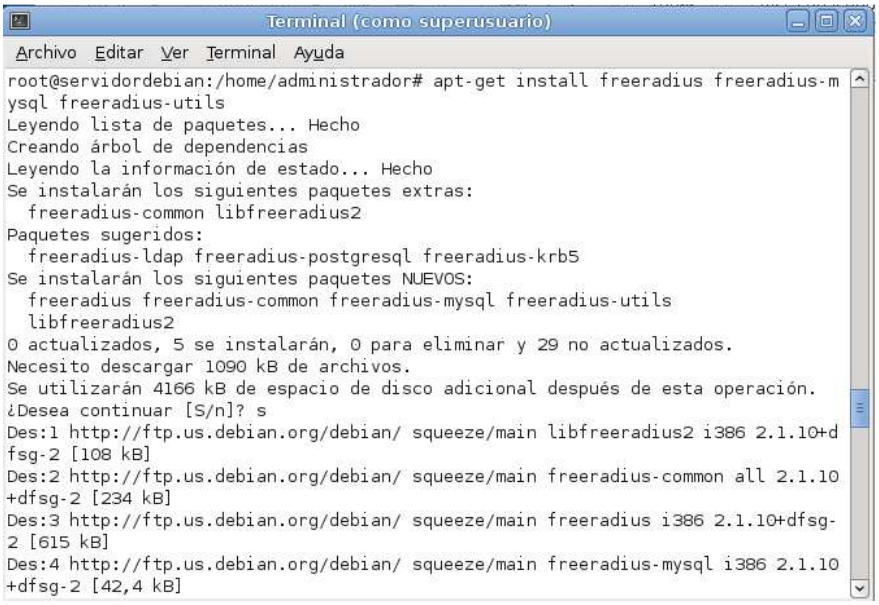


Figura 4.10: Comando para la instalación de Freeradius y sus respectivas herramientas.

Fuente: Autor de la Tesis.

La instalación del servidor Freeradius implica esperar un cierto tiempo, debido a que es necesario instalar varios componentes útiles para su posterior configuración.

Una vez instalado completamente el servidor Freeradius se debe ejecutar, en un terminal de superusuario, las siguientes líneas de comando:

/etc/init.d/freeradius stop (Detiene el demonio de Freeradius)

 # freeradius –X (Verifica la instalación de Freeradius)

Este comando ejecutará el demonio de Freeradius y permitirá que el servidor esté listo para utilizar. Si no hubo fallos en la instalación mostrará el texto mostrado en la Figura 4.11.

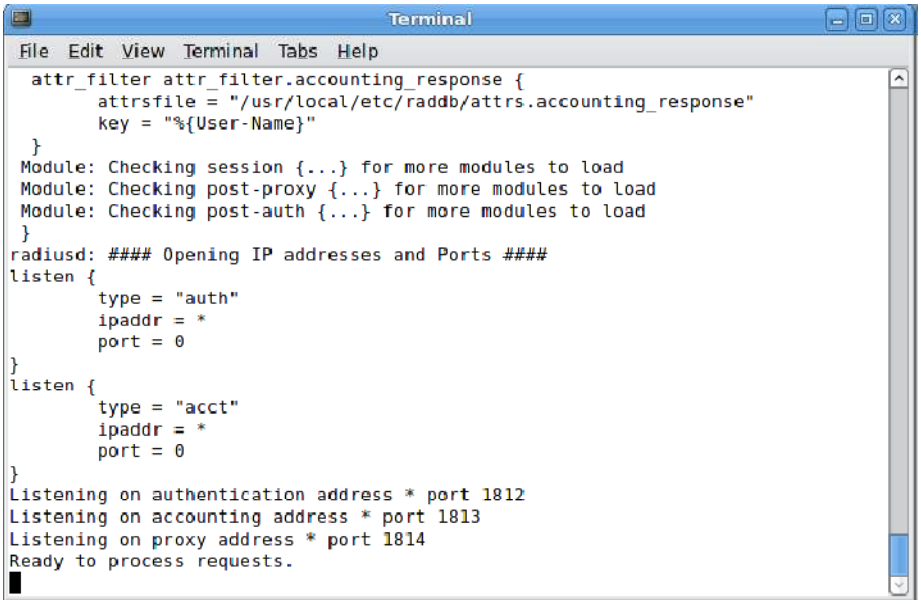


Figura 4.11: Instalación de Freeradius, ejecutar demonio Freeradius para ejecución del servidor Radius.

Fuente: Autor de la Tesis.

Para proceder con la instalación y utilización de Chillispot se debe, primeramente, configurar Freeradius para que trabaje con MySQL además de crear los certificados pertinentes para la autorización de la conexión entre el cliente y el servidor. Dicha configuración será mencionada más adelante en la sección de configuraciones.

4.2.4 INSTALACIÓN DE CHILLISPOT

Se procederá a descargar el paquete Chillispot mediante la instrucción:

 # wget http://www.Chillispot.info/download/chillispot_1.0_i386.deb

El paquete se descargará en el directorio en el cual se está ubicado en es ese momento. La instalación del software que gestionará el portal cautivo deberá ejecutarse para poder utilizar la página de *login* (Registro) que visualizarán los usuarios al ingresar a su navegador, es decir, se utilizará el software Chillispot en el mismo servidor en el cual está instalado Freeradius. Luego de copiar la página de login de Chillispot al servidor apache. Para llevar a cabo este proceso se ejecutará el siguiente comando: *# dpkg –i chillispot_1.0_i386.deb*

Cabe recalcar que este comando se debe ejecutar verificando que el directorio seleccionado sea en el cual se encuentra el paquete descargado de Chillispot.

4.3 CONFIGURACIÓN DE SOFTWARE A UTILIZAR

Una vez instalados todos los tipos de software necesarios, se procederá con la configuración de cada uno de ellos, siendo en su gran mayoría, una configuración tipo edición de archivos.

Para la configuración de cada software a usar se deberá recalcar que la topología implementada es de tipo estrella extendida que utiliza un protocolo Ethernet a una velocidad de 100 Mbps y 1000 Mbps. En esta red se trabaja con el direccionamiento IP clase C: 192.168.10.0 con máscara de red 255.255.255.0 ya que el número de computadores y equipos de conectividad en la red del Colegio San Luis Gonzaga no supera los 254 elementos. Además el direccionamiento dinámico que proveerá Chillispot a los usuarios del portal cautivo estará basado en el rango de direcciones IP 192.168.182.0 con máscara de red 255.255.255.0. En

la Figura 4.12 se distingue el tipo de topología de red y la estructura de conexión que se utilizará para implementar el portal cautivo.

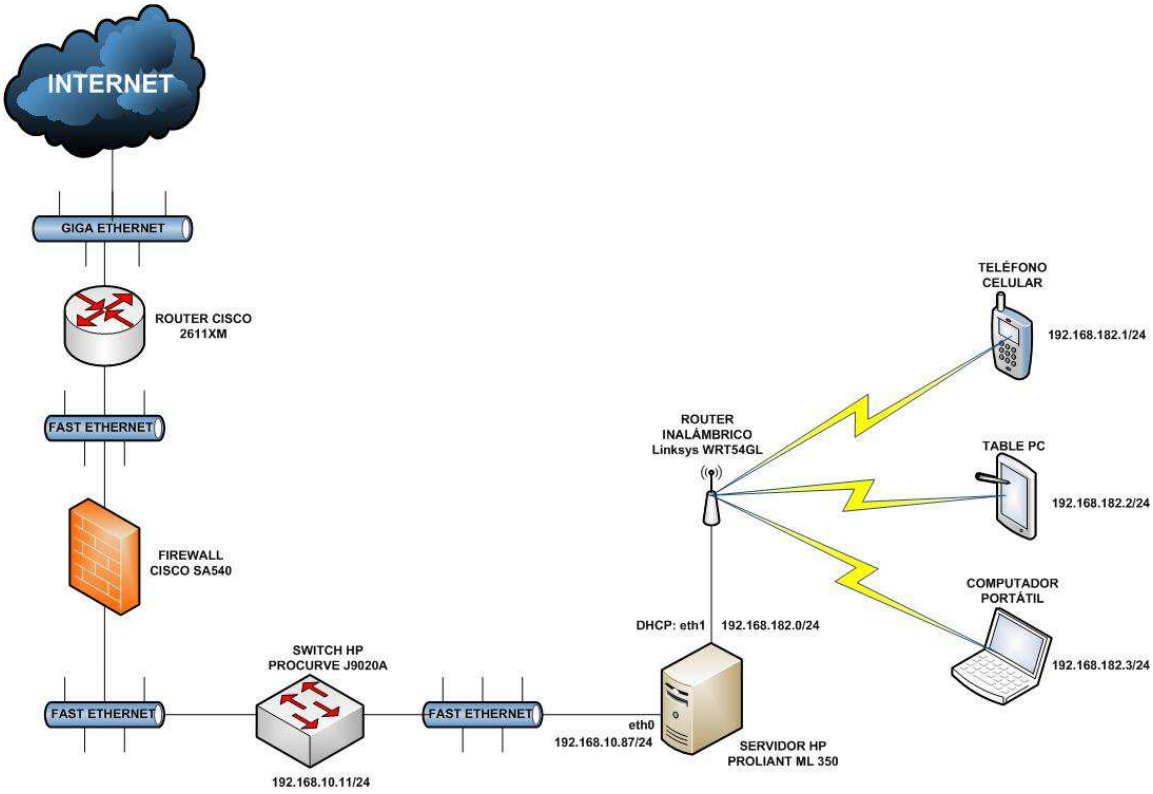


Figura 4.12: Estructura de conexión y comunicación del Portal Cautivo

Fuente: Autor de la Tesis.

La configuración del software tendrá un orden específico, el cual se mencionará a continuación.

4.3.1 CONFIGURACIÓN DE DRIVER TUN/TAP

Si el sistema operativo Debian 6 cuenta con soporte para TUN/TAP se deberá agregar este componente para que inicie al arrancar el sistema operativo. Desde un terminal de superusuario se ejecutará las siguientes líneas de comandos:

 # modprobe tun

 # nano /etc/modules.conf

La línea de comando *#nano /etc/modules.conf* permitirá abrir el archivo *modules.conf* en el cual se deberá agregar la línea “tun”.

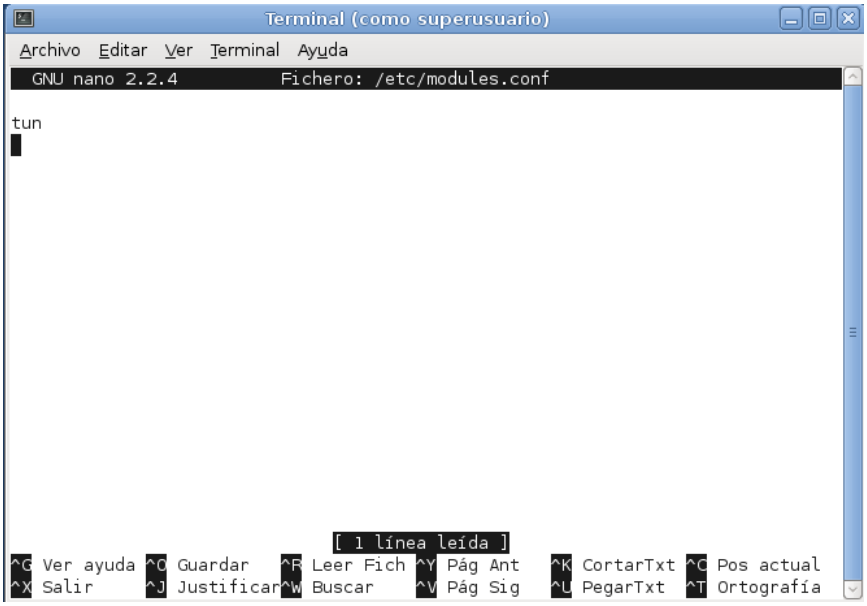


Figura 4.13: Edición de archivo modules.conf

Fuente: Autor de la Tesis.

Al saber que el servidor Freeradius estará trabajando en conjunto con Chillispot, se debe tomar en cuenta que Chillispot adoptará el papel de firewall, por lo que dicho firewall debe tener la capacidad de ejecutar NAT (Network Address Translation) en conjunto con IP Forwarding[28]. Para ejecutar este procedimiento se deberá digitar el comando:

 # echo 1 | sudo tee /proc/sys/net/ipv4/ip_forward

Este comando hará que se cambie el valor de ip_forward de 0 a 1 haciendo las veces de un valor booleano (0=falso y 1=verdadero).

[28] IP Forwarding realiza el reenvío de paquetes IP de una red a otra (en este caso sería de la WAN a unaLAN)

Para concluir con la activación de IP Forward se debe modificar el archivo “sysctl.conf”, se deberá digitar el siguiente comando:

 # nano /etc/sysctl.conf

En este archivo se deberá asegurar que posea la siguiente línea, en el caso de que no esté escrita se la deberá agregar y si se encuentra comentada se la deberá des comentar.

net.ipv4.ip_forward=1

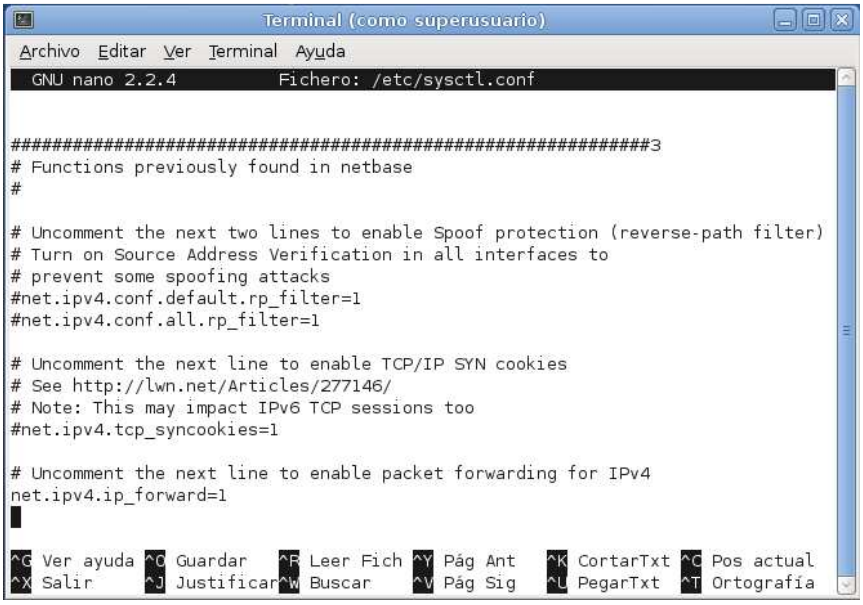


Figura 4.14: Habilitación de net.ipv4.ip_forward en Archivo sysctl.conf

Fuente: Autor de la Tesis.

El correcto funcionamiento del módulo TUN/TAP depende de las dos interfaces de red instaladas en la máquina que funciona como servidor. Recalcando que la interfaz de red **eth0** deberá tener asignada una dirección IP de la red 192.168.10.0/24 que en este caso será la dirección 192.168.10.87/24, la interfaz de red **eth1** deberá estar configurada de tal manera que acepte una dirección IP automáticamente.

4.3.2 CONFIGURACIÓN DE MYSQL

En un terminal de superusuario se debe ingresar a la administración de MySQL con el siguiente comando: *# mysql –u root –p*

Al ejecutar el comando descrito, se deberá digitar la contraseña del usuario root para verificar la identidad de quien administrará el gestor de base de datos. Esta contraseña es la misma que se ingreso al instalar MySQL, en la sección de instalación de software.

Una vez dentro de la administración de MySQL, se deberá crear la base de datos, llamada Radius, que se utilizará para que trabaje con el servidor Freeradius. Para ello se ejecutará el siguiente comando:

mysql> create database radius;

Se creará un usuario para conectar MySQL con el servidor Freeradius, se deberá ejecutar el siguiente comando:

*mysql> grant all on *.* to 'radius'@'localhost' identified by 'gradius;*

- **Grant all on *.*:** otorga permisos globales a todas las bases de datos para el servidor localhost.
- **to 'radius'@'localhost':** Se crea un usuario llamado radius para el servidor localhost.
- **Identified by 'gradius':** Se establece el password gradius para el usuario anteriormente creado.

Para utilizar la base de datos Radius, se deberá importar el esquema de las tablas que trae Freeradius por defecto, esto se llevará a cabo utilizando el siguiente comando: *# mysql –u root – p radius < '/ etc / freeradius / sql / mysql / schema.sql'*

- **mysql –u root –p radius:** Ingresa como usuario root a la base de datos “radius” y copia el archivo mencionado en la dirección propuesta.

- ***‘/ etc / freeradius / sql / mysql / schema.sql’:*** se obtiene el esquema desde el archivo schema.sql ubicado en el directorio /etc/Freeradius/sql/mysql/.

Luego de ejecutar el comando anterior, se deberá ingresar la contraseña del usuario root para MySQL, para confirmar la importación de las tablas del esquema de Freeradius a la base de datos Radius creada en MySQL.

En la Figura 4.15 se muestra la ejecución de cada uno de los comandos mencionados anteriormente con su respectivo resultado.

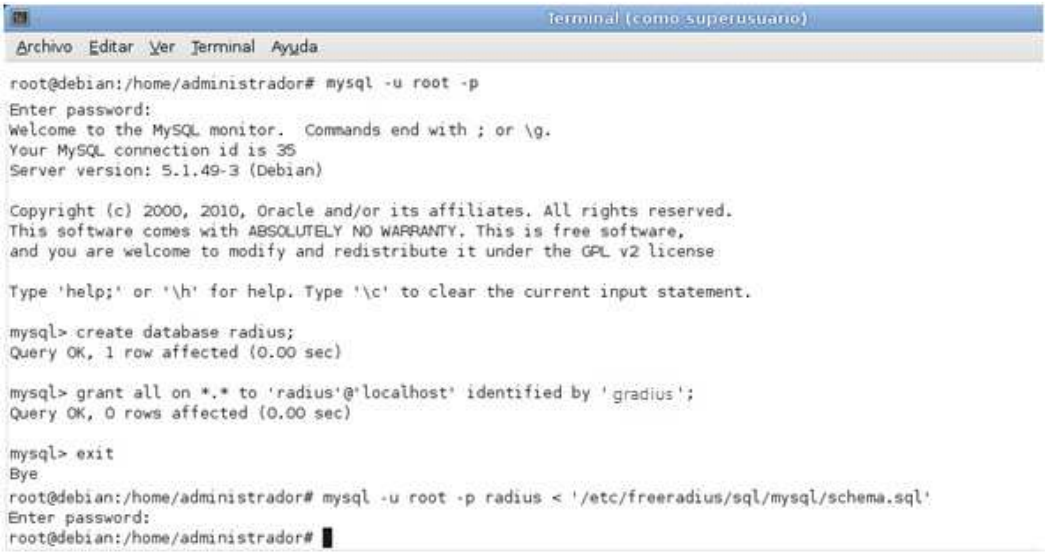


Figura 4.15: Configuración de MySQL para que trabaje en conjunto con Freeradius.

Fuente: Autor de la Tesis.

4.3.3 CONFIGURACIÓN DE FREERADIUS

Para la configuración de Freeradius es importante aclarar que, todos los archivos que se editarán, deberán ser manipulados desde el mismo terminal de superusuario utilizando el comando *nano* seguido de la ruta en la cual se encuentra el archivo necesitado.

Para configurar el servidor Radius se deberá tener ya configurado la base de datos de MySQL, con la que el servidor Radius trabajará conjuntamente para la autenticación y autorización de los usuarios a la red.

Primero se deberá configurar los datos necesarios para que Freeradius se pueda conectar con la base de datos de MySQL, al editar el archivo */etc/freeradius/sql.conf*, en la sección SQL, se establecerá los parámetros de conexión a MySQL:

server = “localhost” El servidor donde está la base de datos

login = “radius” El usuario para conectarse a MySQL

password = “gradius” La contraseña del usuario para conectarse a MySQL

radius_db = “radius” La base de datos que utilizara el servidor Freeradius

Se deberá editar además el archivo */etc/freeradius/clients.conf*. Este archivo contiene las configuraciones para los clientes o redes de clientes que se conectarán al servidor Freeradius. Como primer paso se configurará al cliente “localhost”, este proceso se lo realiza con el fin de hacer pruebas a nivel local, para esto se deberá especificar en la sección *client localhost* el parámetro *secret*, el cual quedará de la siguiente manera:

client localhost { secret = ueslg2011 }

Este parámetro es uno de los datos más importantes en la implementación del Portal Cautivo, ya que es una cadena de caracteres que utilizará tanto Freeradius

como Chillispot para compartir información en el proceso de autenticación y autorización de un usuario. Para la configuración de la palabra secreta se utilizará la cadena de caracteres “ueslg2011”.

También se configurará el archivo ubicado en el directorio /etc/freeradius/sites-available/default, en el cual se deberá habilitar el parámetro “sql” en cada una de las siguientes secciones, de este modo adoptará los parámetros de comunicación con la base de datos a utilizar.

```
authorize {
        preprocess
        chap
        mschap
        suffix
        eap
        sql
                }
-----------------------------
accounting {
        detail
        radutmp
        sql
                }
-----------------------------
session {
        radutmp
        sql
                }
-----------------------------
post-auth {
   sql

                }
```

Este archivo permite que el protocolo AAA (Autenticación, Autorización, Acounting) sea utilizado a través de la base de datos creada en MySQL.

4.3.4 CONFIGURACIÓN DE CHILLISPOT

Una vez realizada la instalación de Chillispot se configurará el archivo chilli.conf ubicado en la dirección /etc/chilli.conf. En este archivo se ingresarán los siguientes parámetros en cada una de las opciones a utilizar, si no se va a utilizar una opción específica es mejor dejarla comentada y así evitar una des configuración del servicio Chillispot:

PARAMETRO	VALOR	DESCRIPCIÓN
net	192.168.10.0/24	Red principal a la cual se van a conectar los usuarios a través del portal cautivo.
dynip	192.168.182.0/24	Rango de direcciones ip's dinámicas (DHCP) las cuales serán otorgadas a los usuarios que se conecten al portal cautivo.
dns1	200.93.216.2	Dirección IP del servidor DNS principal.
dns2	200.93.216.5	Dirección IP del servidor DNS secundario.
radiusserver1	127.0.0.1	Dirección IP del servidor Radius principal.
radiusserver2	127.0.0.1	Dirección IP del servidor Radius secundario.
radiussecret	ueslg2011	Frase secreta de comunicación entre el Servidor Radius y Chillispot.
dhcpif	eth1	Interfaz a través de la cual se proveerán las direcciones automáticamente a través de DHCP.

PARAMETRO	VALOR	DESCRIPCIÓN
uamserver	https://192.168.10.87/ cgi-bin/hotspotlogin.cgi	Dirección en la cual está almacenado el Portal Cautivo.
Uamhomepage	http://192.168.10.87/ hotspotgonzaga/hotspot .html	Pantalla de bienvenida la cual visualizará el usuario al conectarse a la red inalámbrica del Portal Cautivo.
uamsecret	gonzaga	Frase secreta de comunicación entre Chillispot y la página de login.
uamallowed	www.uegonzaga.edu.ec	URL permitidas para su navegación sin tener que iniciar sesión en el portal cautivo.

Tabla 4.1: Parámetros de configuración en el archivo chilli.conf

Fuente: Autor de la Tesis.

Dentro de la documentación de Chillispot se encuentra el archivo "*hotspotlogin.cgi*", este archivo es el que muestra las distintas pantallas al usuario cuando este intente navegar por internet. Para hacer uso de este archivo se deberá primero ubicarlo y descomprimirlo mediante el siguiente comando.

gunzip /usr/share/doc/chillispot/hotspotlogin.cgi.gz

Una vez descomprimido el archivo se lo copia al directorio "cgi-bin", previamente creado en el servidor apache.

 # cp /usr/share/doc/chillispot/hotspotlogin.cgi /var/www/cgi-bin/

Con esta acción ya se dispone de la página a través de la cual el usuario podrá registrarse para poder utilizar el recurso de internet. El mencionado archivo se encuentra editado en lenguaje Perl, pero es posible modificarlo en su parte HTML

para cambiar el aspecto visual de la página que será enviada y vista por el cliente. En este caso no se cambiará el fragmento de programación html, sino que en su lugar se creará una página adicional la cual será la página de bienvenida para los usuarios del HotSpot Gonzaga.

En el archivo hotspotlogin.cgi, copiado en el directorio /var/www/cgi-bin/, se deberá des comentar dos líneas de código, las cuales indican que el portal cautivo utilizará una clave de encriptación y que en la página de login los clientes utilizarán un nombre de usuario y un password para la respectiva autenticación. Para la edición del archivo hotspotlogin.cgi se deberá utilizar la línea de comando:

 # nano /var/www/cgi-bin/hotspotlogin.cgi

Las líneas a descomentar son las mostradas en la Figura 4.16.

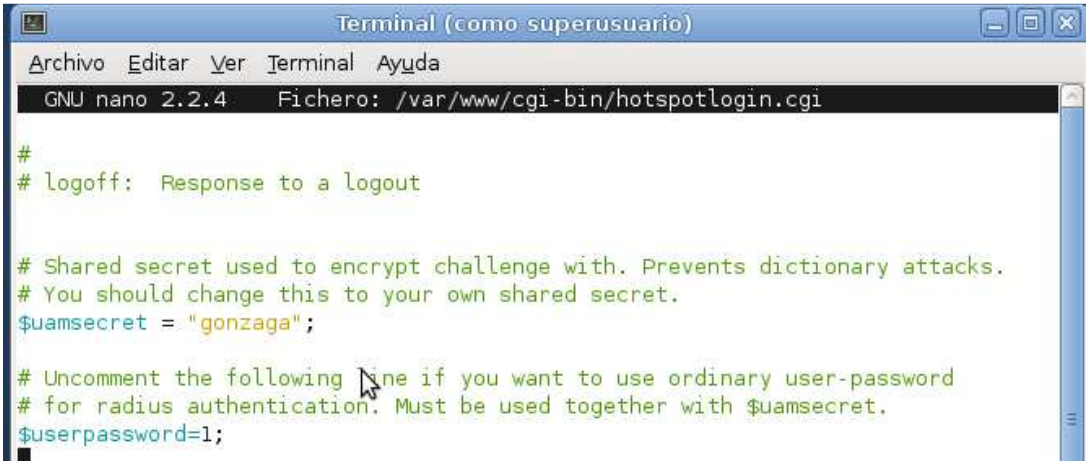


Figura 4.16: Descomentar líneas de programación uamsecret y userpassword en el archivo hotspotlogin.cgi

Fuente: Autor de la Tesis.

En el parámetro $*uamsecret* se le asigna la palabra “gonzaga” para establecer que esa será la clave con la cual se encriptarán los datos del usuario, y en el

parámetro $*userpassword* se verifica que esté asignado el número 1 para habilitar el ingreso del nombre de usuario y contraseña.

Para diseñar la página que será la bienvenida a los usuarios, se utilizará código HTML y la inserción de imágenes alusivas al Colegio San Luis Gonzaga y a los distintos tipos de software utilizados en el proceso de implementación del HotSpot Gonzaga. En dicha página se muestra información del HotSpot Gonzaga junto a las Condiciones y Recomendaciones de Uso.

La página de bienvenida a HotSpot Gonzaga también estará alojada en el servidor Apache, por lo que se deberá crear un directorio que guarde las imágenes y el archivo html. En este caso se tiene el directorio /var/www/hotspotgonzaga.

En la Figura 4.17 se muestra la página de bienvenida para los usuarios que accedan a HotSpot Gonzaga.

Figura 4.17: Página de bienvenida para los usuarios de HotSpot Gonzaga.

Fuente: Autor de la Tesis.

El enlace del botón Ingresar es http://192.168.182.1:3990/prelogin, se usa esta dirección porque una vez que el cliente obtiene una dirección IP del servicio

Chillispot, la puerta de enlace por defecto se convierte en la dirección 192.168.182.1 y utiliza el puerto 3990 para una conexión segura hacia la página prelogin en donde el usuario ingresa sus datos para la verificación en el servidor Freeradius.

4.3.5 CONFIGURACIÓN DEL ROUTER INALÁMBRICO CISCO LINKSYS WRT160NL

La implementación del portal cautivo requiere configurar un router inalámbrico de tal manera que utilice la aplicación Chillispot y de este modo ejecute la acción de autenticador para los usuarios que requieran conectarse a la red a través del mencionado portal cautivo. Se utilizará una primera configuración del router inalámbrico, con la que se realizará la Prueba Práctica 2, utilizando la siguiente parametrización:

En el router inalámbrico se deberá establecer que:

- El router inalámbrico trabajará en un modo inalámbrico AP (Access Point – Punto de Acceso).
- Definir un modo mixto para el estándar de la red inalámbrica, esta configuración trabajará con el estándar 802.11b y 802.11g, manteniendo la frecuencia de 2.4 GHz y una velocidad de transmisión que oscile entre los 11 Mbps y los 54 Mbps.
- Conceder un nombre a la red inalámbrica (SSID[29]), el cual será difundido a todos los clientes inalámbricos que deseen conectarse a la red mediante un canal inalámbrico estándar. Por defecto tiene asignado el canal número 6 de 2.437 GHz, se configurará la opción Auto, de este modo identificará automáticamente la frecuencia de transmisión mas óptima.

[29] Service Set IDentifier (SSID): es un nombre incluido en todos los paquetes de una red inalámbrica para identificarlos como parte de esa red. Todos los dispositivos inalámbricos que intentan comunicarse entre sí deben compartir el mismo SSID

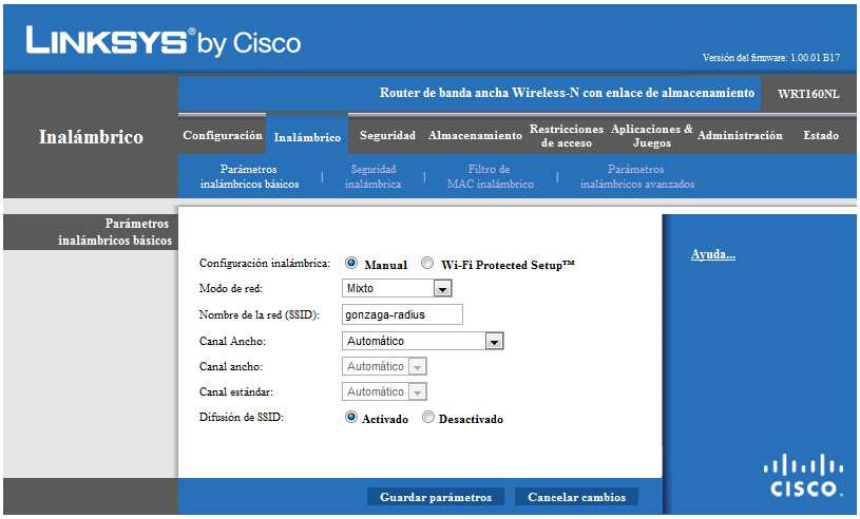


Figura 4.18: Configuración del nombre de la red inalámbrica (SSID).

Fuente: Autor de la Tesis.

Cuando se disponga de un nombre de red se procederá a configurar la seguridad de la misma. En este caso, el modo de seguridad de red se encontrará desactivado, debido a que la administración de la seguridad para la red y para los usuarios es proporcionada por el servidor Freeradius.

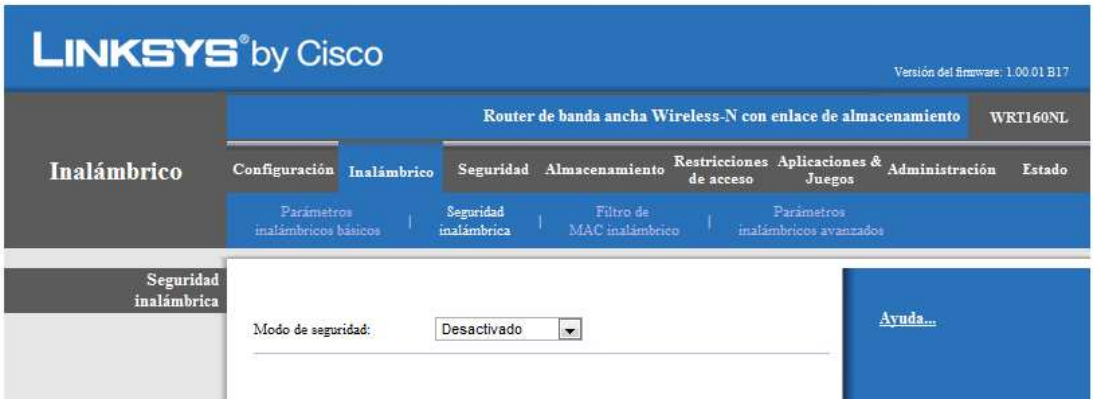


Figura 4.19: Configuración del modo de seguridad en el router inalámbrico.

Fuente: Autor de la Tesis.

Para la Tercera Prueba Práctica, es importante deshabilitar el servicio DHCP que ofrece el router inalámbrico, ya que quien asigna las direcciones IP es el servicio Chillispot alojado en el servidor. El router inalámbrico se deberá conectar a la interfaz de red del servidor Freeradius denominada eth1.

Con la mencionada configuración se tendrá en orden lo requerido para poder montar el Portal Cautivo, para la publicación del mencionado Portal se requerirá cambiar el aspecto de la página de bienvenida y modificar el texto de la página de autenticación.

La configuración de cada uno de los programas implicados en la implementación del HotSpot se deberá realizar según las necesidades y conveniencias de la o las personas que vayan a hacer uso del Portal Cautivo. Pero si fuese el caso, la configuración ya mostrada es la base fundamental del trabajo que se puede realizar para que el HotSpot funcione adecuadamente.

CAPÍTULO 5

PRUEBAS Y RESULTADOS

Para comenzar con la implementación práctica del portal cautivo, se deberá realizar las pruebas necesarias que guiarán dicha implementación. Se realizará tres pruebas prácticas para verificar el correcto desempeño de los distintos tipos de software y hardware.

5.1 PRIMERA PRUEBA PRÁCTICA

La primera prueba práctica consiste en probar la conexión entre el servidor Freeradius y el servidor de base de datos MySQL. Para esta prueba se deberá crear un nuevo usuario en la base de datos “radius”, en este caso se utilizó los datos mostrados a continuación:

- **Username:** angel
- **Atribute:** Cleartext-Password
- **Op:** :=
- **Value:** angel

Para lo cual se deberá ejecutar los siguientes comandos:

- Ingresar a la base de datos: # *mysql –u root –p*
- Escribir la contraseña de MySQL: *root*
- Usar la base de datos radius: *mysql> use radius;*
- Insertar el nuevo usuario a la base de datos:
- *INSERT INTO `radcheck` (`username `, `attribute`,`op`,`value`) VALUES (‘angel’,’Cleartext-Password’,’:=’,’angel’)*

- Verificar si el usuario está creado: *mysql> SELECT * FROM radcheck;*

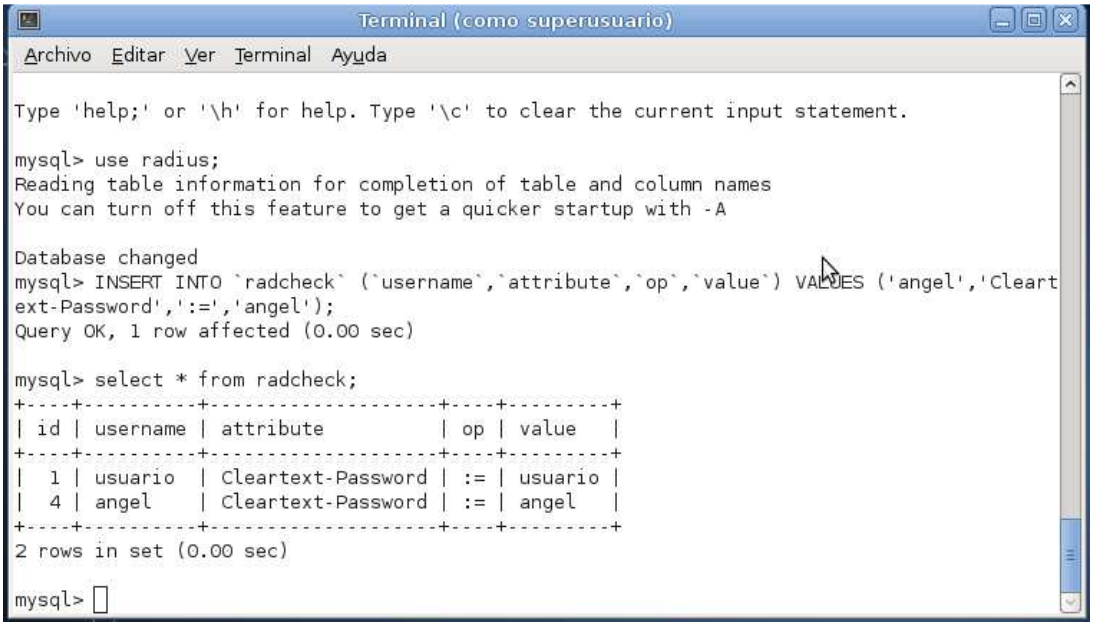


Figura 5.1: Ingreso y consulta de nuevo usuario en MySQL.

Fuente: Autor de la Tesis.

La primera prueba práctica consiste en comprobar que se esté autenticando a los usuarios almacenados en la base de datos mediante la siguiente instrucción:

 # radtest usuario password localhost 1812 password_secreto_compartido

El resultado obtenido es que al aceptar los paquetes de información se comprueba que la conexión entre el servidor Freeradius y el servidor MySQL está activa y funcional. La Figura 5.2 muestra el resultado de la prueba.

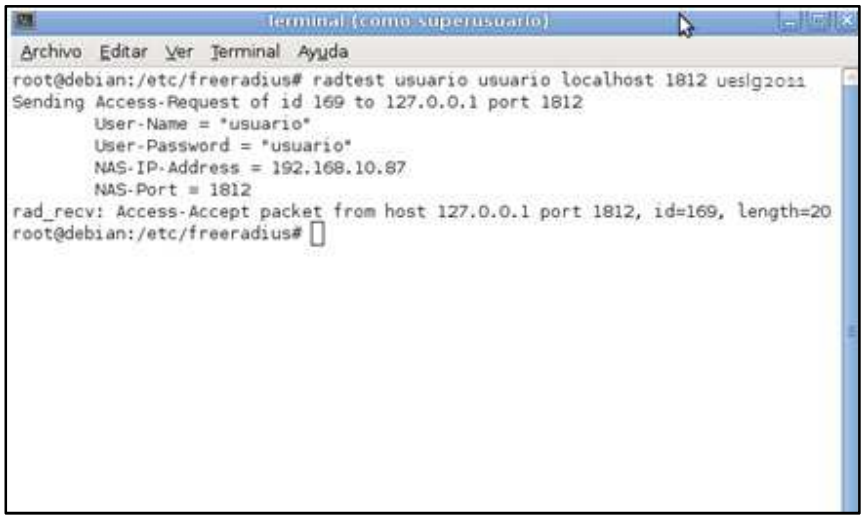


Figura 5.2: Prueba de conexión entre Freeradius y MySQL ejecutado desde un terminal.

Fuente: Autor de la Tesis.

Para realizar las siguientes pruebas prácticas se deberá establecer una configuración propia para la red inalámbrica que será utilizada en el Colegio San Luis Gonzaga en conjunto con el servidor Freeradius y conocer el diagrama de conexión que se manejará para la implementación del Portal Cautivo.

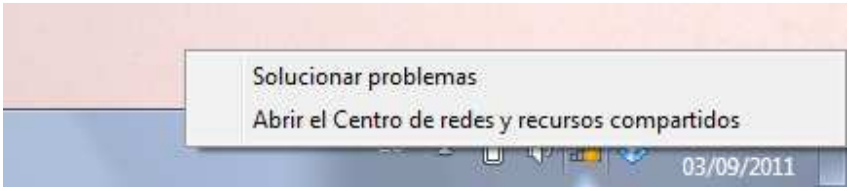
5.2 SEGUNDA PRUEBA PRÁCTICA

Cabe recalcar que la conexión y configuración que se utilizará a partir de esta segunda prueba práctica, está descrita en el CAPITULO 4 en el Tema 4.3.5 Configuración del Router Inalámbrico CISCO Linksys WRT160NL

La segunda prueba práctica consistirá en probar la conexión desde un usuario con un dispositivo inalámbrico hasta el servidor Freeradius pero sin pasar a través del portal cautivo. Para ejecutar la segunda prueba práctica se necesitará utilizar el módulo de autenticación en un servidor RADIUS desde el propio router inalámbrico, manejando la configuración del Router Linksys WRT160NL mostrada en el Tema 4.3.5.

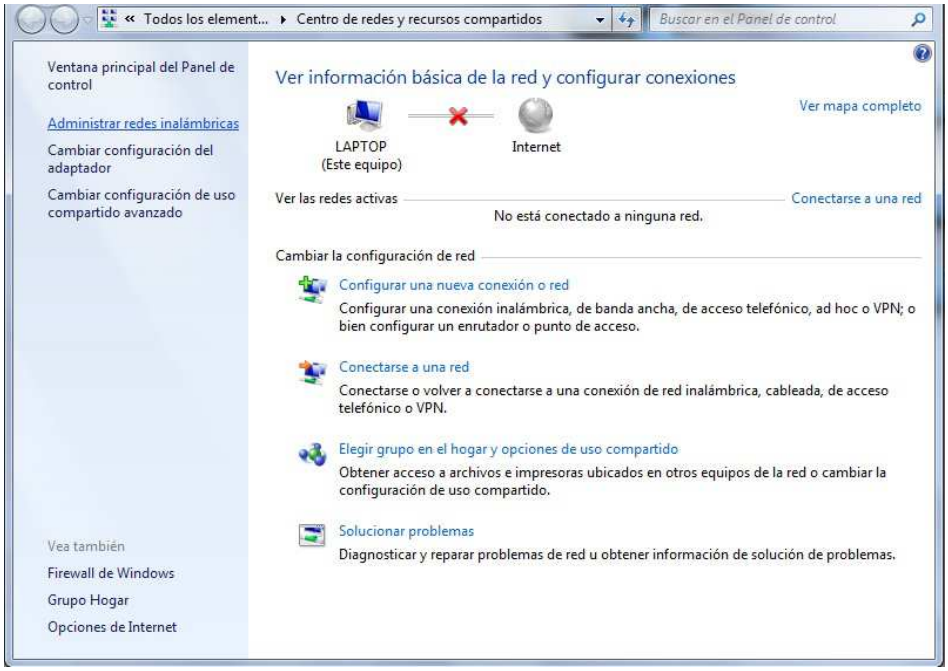
Con la configuración ya establecida tanto en el servidor Freeradius como en el Router Inalámbrico, se conectará un cliente (computador portátil) para probar la autenticación desde la base de datos gestionada en MySQL. Se utilizará un equipo portátil con Sistema Operativo Windows 7, en el cual se realizarán las siguientes configuraciones:

Se abrirá la ventana de Centro de redes y recursos compartidos.



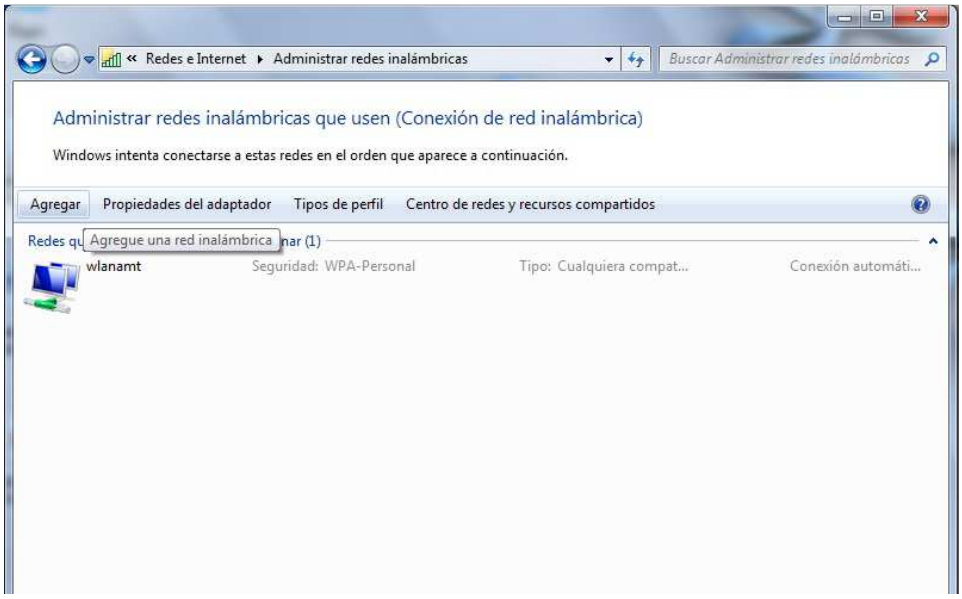
(A)

Seleccionar la tarea “Administrar redes inalámbricas”.

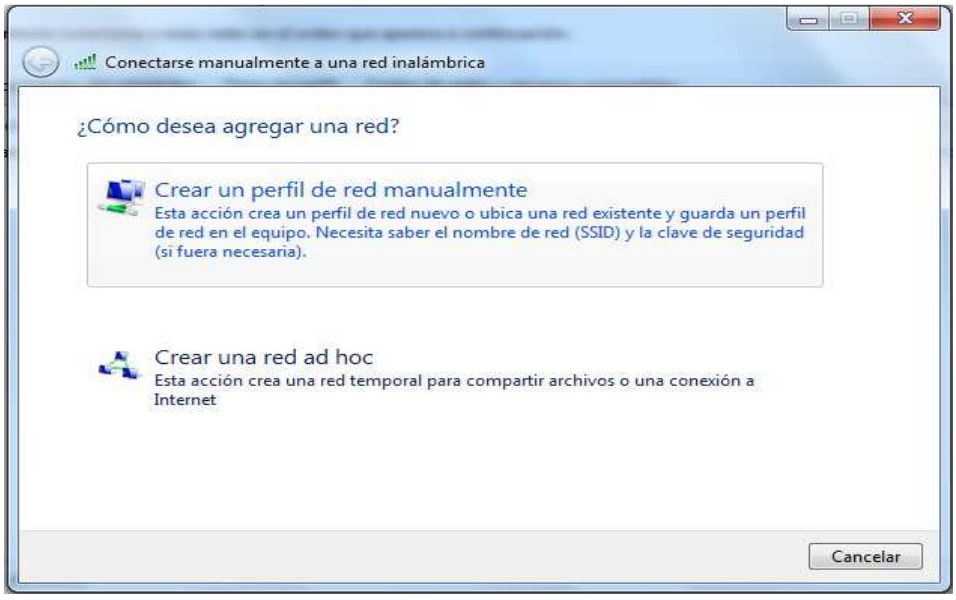


(B)

Se deberá agregar un nuevo perfil de red haciendo clic en el botón “Agregar”, para posteriormente añadir un perfil de red manualmente.



(C)

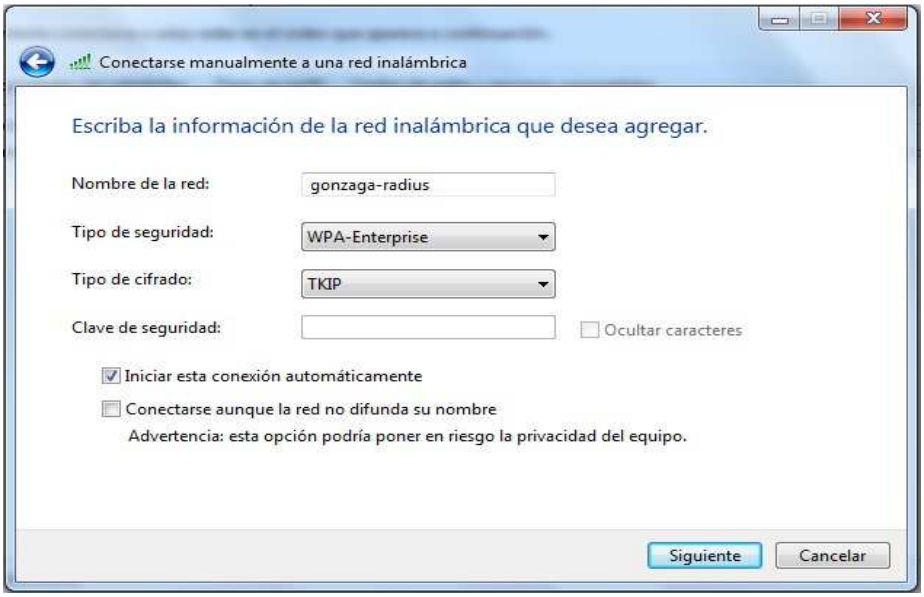


(D)

Se establecerá los siguientes parámetros para la nueva red inalámbrica, estos parámetros serán utilizados para pruebas posteriores y serán base del funcionamiento final del Portal Cautivo.:

- Nombre de la Red: gonzaga-radius

- Tipo de seguridad: WPA-Enterprise
- Tipo de Cifado: TKIP



(E)

Figura 5.3 Creación de Red gonzaga-radius para ejecución de pruebas prácticas

(A) Centro de Recursos de Red.

(B) Ventana de Centro de recursos compartidos.

(C) Ventana de Administración de Redes Inalámbricas.

(D) Ventana para agregar un perfil de red manualmente.

(E) Ventana de parametrización para red inalámbrica que se desea agregar.

Fuente: Autor de la Tesis

Al hacer clic en botón siguiente se desplegará la información de que se agregó correctamente la red gonzaga-radius, y se deberá presionar en el botón cerrar.

Seleccionar el nuevo perfil de red creado y hacer clic derecho escogiendo la opción “Propiedades”. Desde la pestaña “Seguridad” se configurará el modo de autenticación y el método de autenticación de la red.

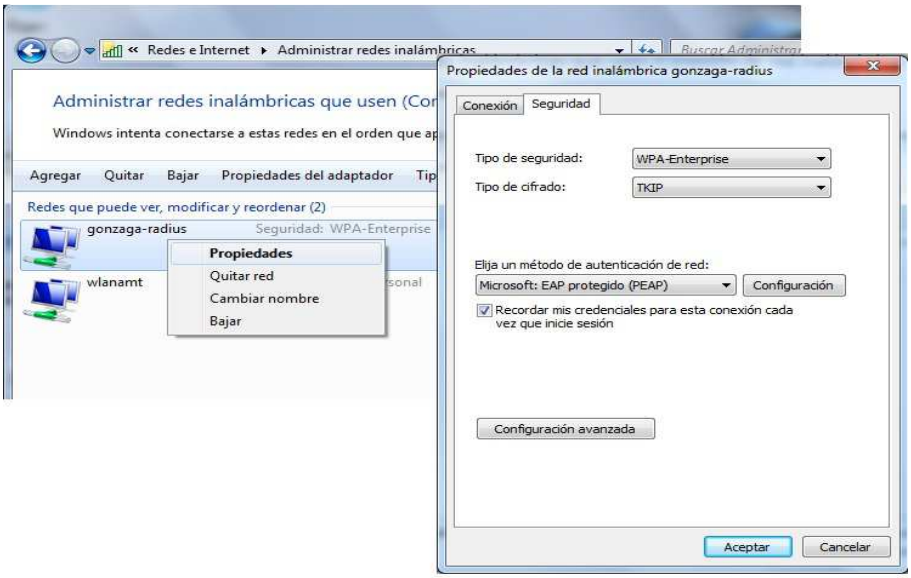


Figura 5.4: Ventana de configuración de las propiedades de la red gonzaga-radius.

Fuente: Autor de la Tesis.

Para el primer caso se deberá desmarcar la opción “Recordar mis credenciales para esta conexión cada vez que inicie sesión” y presionar sobre el botón “Configuración Avanzada”. Seguidamente se deberá marcar la casilla de “Especificar modo de autenticación” y escoger la opción de “Autenticación de usuarios”. Se deberá aceptar todos los cambios realizados presionando sobre el botón “Aceptar”.

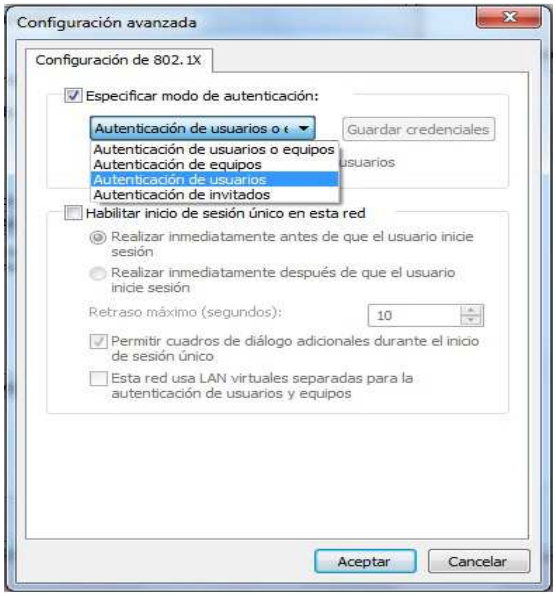


Figura 5.5: Ventana de especificación de modo de autenticación.

Fuente: Autor de la Tesis

Ahora presionando sobre el botón “Configuración” en la pestaña “Seguridad” se deberá indicar que al momento de conectarse a la red creada, no valide un certificado de servidor, por lo que se debe desmarcar la casilla de “Validar un certificado de servidor”

Figura 5.6: Ventana de verificación para la validación de un certificado de servidor.

Fuente: Autor de la Tesis.

Posteriormente, para configurar el método de autenticación, se deberá ingresar a la configuración del tipo de contraseña segura a utilizar, se debe tener en cuenta que esté habilitado la opción “Contraseña segura (EAP-MSCHAP v2)” y presionar en el botón “Configurar”.

Se deberá desmarcar la opción de “Usar automáticamente el nombre de inicio de sesión y la contraseña de Windows”, con esto se obliga al usuario a escribir su nombre de usuario y contraseña asignada desde el servidor MySQL.

Una vez parametrizado el modo y método de autenticación se debe aceptar todos los cambios realizados presionando el botón “Aceptar”.

En la esquina inferior derecha de la pantalla del cliente Windows aparecerá un mensaje pidiendo información adicional para conectarse con la red que se creó anteriormente, haciendo un clic sobre el cuadro de dialogó aparecerá una nueva ventana indicando que se deberá ingresar las credenciales de usuario para poder conectarse a la red gonzaga-radius.

(A)

(B)

Figura 5.7: Ingreso de información de usuario para conexión con red gonzaga-radius

(A) Cuadro de dialogo que muestra mensaje de "Se necesita información adicional para conectarse a gonzaga-radius".

(B) Ventana de ingreso de credenciales de usuario para conectarse a gonzaga-radius.

Fuente: Autor de la Tesis.

La información digitada es enviada al servidor Radius, el mismo que hace una petición a la base de datos preguntando si existe el usuario que está pidiendo la solicitud de conexión, la base de datos puede responder con dos posibilidades: una respuesta afirmativa o una respuesta negativa en cuanto a la existencia del usuario en cuestión. Si se verifica la existencia de los datos de usuario, el servidor Radius envía un Access-Accept; de lo contrario el mismo servidor niega el acceso del usuario a la red.

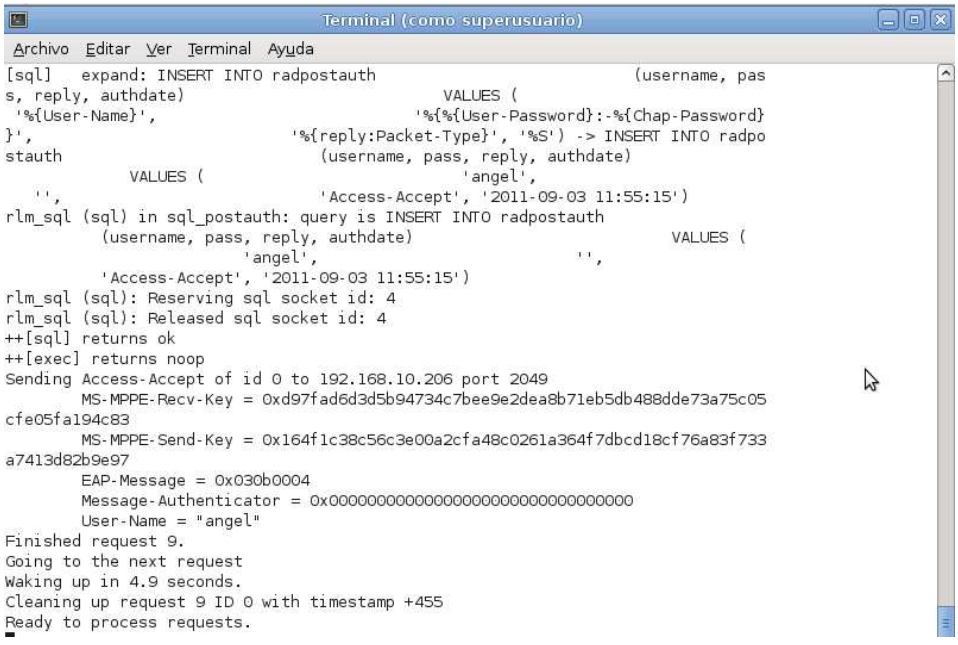


Figura 5.8: Terminal root en Debian informando de "Acceso Aceptado" desde el servidor Freeradius.

Fuente: Autor de la Tesis.

En el cliente Windows aparecerá un mensaje de: “gonzaga-radius Acceso a Internet”

Figura 5.9: Ventana de información en el proceso de conexión a gonzaga-radius y posterior conexión exitosa con acceso a internet.

Fuente: Autor de la Tesis.

5.3 TERCERA PRUEBA PRÁCTICA

Para la tercera prueba práctica se establecerá la conexión entre el servidor Freeradius y un cliente inalámbrico pero a través del portal cautivo proporcionado por el servicio de Chillispot; se utilizará el mismo esquema mostrado en la Figura 1.7. El fin de esta prueba es proveer de internet al usuario que verifique su identidad como cliente del servidor Freeradius. Se debe recordar que en esta prueba es preciso utilizar la configuración mostrada en el Tema 4.3.5.

Se utilizará un computador portátil con sistema operativo Windows 7 y se efectuará la prueba en el siguiente orden:

1. Configurar la tarjeta de red inalámbrica del computador portátil para que obtenga una dirección IP automáticamente. Habilitar DHCP para la NIC inalámbrica.
2. Verificar la disponibilidad de la red inalámbrica “gonzaga-radius” y conectarse a la misma.

Figura 5.10: Verificación de disponibilidad de la red inalámbrica "gonzaga-radius".

Fuente: Autor de la Tesis.

3. En este punto, el computador portátil ya estará conectado a la red inalámbrica y adoptará una dirección IP perteneciente a la red 192.168.182.0 establecido en la configuración de Chillispot en el archivo chilli.conf.

Figura 5.11: Asignación de Dirección IP para dispositivo inalámbrico de usuario.

Fuente: Autor de la Tesis.

4. Es posible que aparezca un mensaje de advertencia indicando que para la red a la que se ha conectado el usuario necesita información adicional para poder utilizarla en su totalidad.

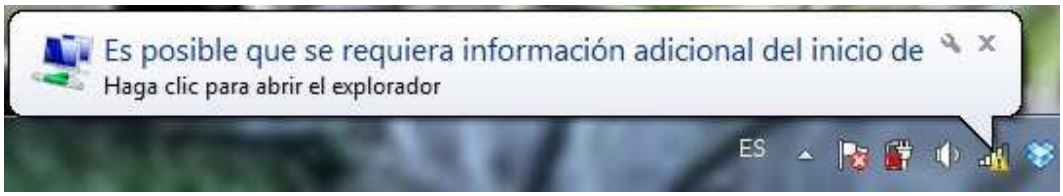


Figura 5.12: Mensaje informativo para incluir nombre de usuario y contraseña en la red "gonzaga-radius".

Fuente: Autor de la Tesis.

5. Ahora al abrir un navegador de internet, automáticamente el usuario será re direccionado a la página de bienvenida del portal cautivo (http://192.168.10.87/hotspotgonzaga/hotspot.html).

Figura 5.13: Página de Bienvenida para el HotSpot Gonzaga.

Fuente: Autor de la Tesis.

6. Presionando en el botón “Ingresar”, se reubicará al usuario en la página de Login del HotSpot Gonzaga. En la página mostrada se deberá ingresar el nombre de usuario y contraseña asignados para un cliente de la red inalámbrica.

Figura 5.14: Visualización del Portal Cautivo Gonzaga y posterior ingreso de datos de usuario para utilizar el recurso de internet.

Fuente: Autor de la Tesis.

7. Se visualizará una ventana tipo pop-out que muestra el tiempo de conexión transcurrido desde el ingreso del usuario y la opción “Logout” para la desconexión del HotSpot Gonzaga. Es importante que el usuario mantenga abierta esta ventana durante el tiempo que permanezca conectado, ya que así podrá asegurar un cierre de sesión correcto.

Figura 5.15: Ventana de Informe de Estado de Logueo de HotSpot.

Fuente: Autor de la Tesis.

Como resultado de la implementación del portal cautivo se puede obtener una medición de los usuarios que ingresaron a la red inalámbrica del Colegio Gonzaga a través del portal cautivo y el tiempo que estuvieron conectados al servicio. Este tipo de reporte se lo obtiene a partir del administrador de base de datos utilizando el software PhpMyAdmin, en la base de datos “Radius”, específicamente de la tabla “Radcheck”. Al obtener este tipo de información se podrá controlar la cantidad de accesos al portal cautivo en una hora específica, característica de conexión al hotspot muy importante para establecer la efectividad del Portal Cuativo.

Se adjunta en el Anexo 2 un reporte obtenido desde la base de datos mencionada con los usuarios que ingresaron al portal cautivo.

Con la realización de las tres pruebas prácticas se ha configurado y probado que la implementación del portal cautivo del Colegio San Luis Gonzaga se ha dado de manera secuencial y verificando cada una de las distintas fases de la conexión que se da entre un usuario con un dispositivo inalámbrico y el servidor de autenticación. Con este capítulo se da por concluido el diseño, configuración e implementación del Portal Cautivo para el Colegio San Luis Gonzaga.

CAPÍTULO 6

CONCLUSIONES Y RECOMENDACIONES

6.1 CONCLUSIONES

- El control del ingreso de los usuarios al servicio del internet se puede administrar y cuantificar, por lo que es posible adoptar nuevas políticas de uso según se vaya trabajando en el Portal Cautivo del Colegio San Luis Gonzaga.

- El Portal Cautivo del Colegio San Luis Gonzaga permite utilizar una encriptación básica de los datos de los usuarios que viajan en la red inalámbrica para el uso del internet a un nivel de tipo académico, esta implementación de seguridad en la institución es suficiente en cuanto al nivel de seguridad planteada. Este tipo de soluciones en cuanto a seguridad de redes no son tan viables en empresas o instituciones que requieran un alto nivel de seguridad y protección para los datos de los usuarios, para lo cual se cuenta con distintos tipos de soluciones de hardware y software a una escala mucho mayor.

- La restricción y administración de los sitios web permitidos para el Colegio San Luis Gonzaga se lo realizó en conjunto con un Firewall Cisco el cual administra la red utilizando WebFilters y limitadores de ancho de banda.

- Chillispot no ofrece la opción de limitaciones de tiempo para los usuarios conectados al Portal Cautivo, pero la configuración actual está totalmente acorde con la política del Colegio San Luis Gonzaga de que el servicio de internet esté libre por ser un servicio meramente de investigación y con esta

premisa no se debería limitar el tiempo de la indagación de conocimientos e información académica.

- Al trabajar en conjunto los distintos tipos de software, proveen de total disponibilidad e integridad del servicio en cuanto a la conectividad de red a través del portal cautivo para los usuarios de la Red Inalámbrica del Colegio San Luis Gonzaga.

- Al centralizar la instalación de todos los programas en un mismo servidor físico, la comunicación entre el software de autenticación y el software de administración de usuarios, se ejecuta más efectivamente, debido a que utiliza el ancho de banda del bus de datos propio del servidor implementado, asegurando una respuesta mucho más rápida de la verificación de los datos del usuario.

- El control administrativo del portal cautivo es totalmente adaptable a una red específica, por lo que su implementación resulta bondadosa en cuanto a costo/beneficio, debido a su bajo costo de implementación y gran utilidad para el control de los usuarios de una wlan.

6.2 RECOMENDACIONES

- Se recomienda que dentro del data center del Colegio San Luis Gonzaga se pueda incluir un servidor dedicado, con el cual se pueda obtener todas las prestaciones de un equipo especial para soportar el tráfico de datos, tanto para las peticiones de los usuarios hacia el servidor Freeradius, como para los datos de retorno que el servidor ofrece al beneficiario de la autenticación y autorización.

- Como resguardo a los datos almacenados, a la configuración establecida dentro del servidor y del router inalámbrico, es recomendable conectar la alimentación de energía eléctrica a un UPS (Sistema de Alimentación Ininterrumpida) de 120V, 650VA, debido a una inestabilidad en el flujo de corriente en los predios del Colegio San Luis Gonzaga.

- Como la utilización del portal cautivo será masiva dentro del estudiantado, la inserción de los usuarios y sus respectivos passwords para el acceso y posterior verificación dentro de la base de datos, no se deberá realizar mediante instrucciones SQL, por lo cual se podría implementar una interfaz básica diseñada en lenguaje PHP para ingresar un usuario y su respectiva contraseña, si se necesitara ingresar una lista de usuarios se recomienda utilizar PhpMyAdmin y subir los datos necesarios en conjunto a través de un archivo CSV creado en Microsoft Excel.

- Al manejar datos de usuarios y configuraciones, se recomienda crear un plan de respaldo de información en futuras implementaciones de características adicionales en el Portal Cautivo del Colegio San Luis Gonzaga.

- Verificar que la versión del software a instalar sea la más actual, de este modo se podrá utilizar la mayor cantidad de características de configuración y disponibilidad de los servicios, para una futura escalabilidad en la implementación de un HotSpot.

- En cuanto al software Chillispot se recomienda en un futuro utilizar su actualización CoovaChilli o el protocolo Diameter, no se mencionó en el presente proyecto debido a su poco uso y poca cantidad de información.

BIBLIOGRAFÍA

TEXTOS

Arakhne. «Manual de Instalación.pdf.» p. 3. <http://www.cpto.org/arakhneinstal.pdf>.

CHILIQUINGA LLIVE, Edison. «Análisis, Diseño y Prototipo de una red inalámbrica de acceso a Internet.» 2007. <http://bibdigital.epn.edu.ec/bitstream/15000/744/1/CD-1137.pdf>.

DURÁN, Miguel. El museo de los 8 bits. 10 de Febrero de 2008. <http://www.museo8bits.es/wiki/index.php/IEEE_802.11>.

ENCISO ROCHA, Hollman. «Implementación de un prototipo de red WMAN utilizando topología MESH para el intercambio de contenido e información con el protocolo NTK.» 2008. Universidad de San Buenaventura . <http://www.slideshare.net/hollmanenciso/tes>.

GARCÍA, Cristian y Otros. «Portal Cautivo PF Sense.» 2010. Chile. <http://www.slideshare.net/valericio1/portal-cautivo.>.

GODMOL. «VPN ¿Qué es y cómo se crea una VPN?» 8 de Junio de 2007. <http://www.configurarequipos.com/doc499.html>.

NAVARRO, Vicente. « Los canales Wi-Fi en la banda de 2.4GHz (802.11b/g).» 2011. < http://www.vicente-navarro.com/blog/2008/04/26/los-canales-wi-fi-en-la-banda-de-24ghz-80211bg/>.

TORTOSA CERVERA, Carlos. Seguridad en Redes Inalámbricas. Universidad de Valencia, 2005.

Universidad Politécnica de Valencia, Instalación y Configuración de un Servidor RADIUS. «Grupo de Redes de Computadoras.» Enero de 2012. Instalación y Configuración de un Servidor RADIUS. <http://www.grc.upv.es/docencia/tra/PDF/Radius.pdf>.

PÁGINAS WEB

- http://www.monografias.com/trabajos18/protocolo-wep/protocolo-wep.shtml
- http://www.worldlingo.com/ma/enwiki/es/AAA_protocol
- http://www.configurarequipos.com/doc499.html
- http://www.uv.es/siuv/cas/zxarxa/vpn.htm
- http://dns.bdat.net/seguridad_en_redes_inalambricas/x59.html
- http://www.oas.org/en/citel/infocitel/2006/junio/wifi_e.asp

- http://www.freebsd.org/doc/es/books/handbook/network-dhcp.html
- http://www.debian.org/releases/stable/i386/ch03s04.html.es
- http://usemoslinux.blogspot.com/2011/02/debian-6-squeeze-liberado.html
- http://www.openssl.org/
- http://www.chillispot.info/
- http://packages.debian.org/es/sid/dpkg-dev
- http://nullpointerexception.tk/pahko/2011/01/10/instalar-phpmyadmin-en-archlinux/
- http://www.phpmyadmin.net/home_page/index.php
- http://www.virusprot.com/cursos/redes-inal%c3%a1mbricas-curso-gratis10.htm

ANEXOS

ANEXO 1 - ARCHIVO DE CONFIGURACIÓN PARA EL SERVIDOR RADIUS

ARCHIVO DE CONFIGURACIÓN PARA FREERADIUS RADIUSD.CONF

En el Anexo 1 se explicará la funcionalidad del código descrito.

En esta sección se configura la utilización del archivo clients.conf, incluyéndolo en ejecución del archivo principal radiusd.conf. Es incluido debido a que ahí se configuró el Access Point por el cual los usuarios se conectarán a la red inalámbrica.

```
# CLIENTS CONFIGURATION
#
#  Client configuration is defined in "clients.conf".
#
#  The 'clients.conf' file contains all of the information from the old
#  'clients' and 'naslist' configuration files.  We recommend that you
#  do NOT use 'client's or 'naslist', although they are still
#  supported.
#
#  Anything listed in 'clients.conf' will take precedence over the
#  information from the old-style configuration files.
#
$INCLUDE clients.conf
```

En la sección de configuración de módulos, se des comenta las líneas en donde se incluye a los archivos: sql.conf y eap.conf, dando lugar a que el servidor Freeradius se pueda conectar a la base de datos.

```
# MODULE CONFIGURATION
#  The names and configuration of each module is located in this section.
#  After the modules are defined here, they may be referred to by name,
#  in other sections of this configuration file.
#
modules {
        #
        #  Each module has a configuration as follows:
        #       name [ instance ] {
        #               config_item = value
        #       }
        $INCLUDE ${confdir}/modules/
        #  Extensible Authentication Protocol
        #  For all EAP related authentications.
        #  Now in another file, because it is very large.
        $INCLUDE eap.conf
        #  Include another file that has the SQL-related configuration.
        #  This is another file only because it tends to be big.
        $INCLUDE sql.conf
        #  This module is an SQL enabled version of the counter module.
        $INCLUDE sql/mysql/counter.conf
        #  IP addresses managed in an SQL table.
        #$INCLUDE sqlippool.conf
}
```

Este segmento de código representa el tiempo durante el cual un usuario esta registrado y el periodo durante el cual puede hacer uso de la conexión a través del Portal Cautivo. Siendo este último un periodo diario.

```
#  The expression module doesn't do authorization,
#  authentication, or accounting.  It only does dynamic
#  translation, of the form:
#
#          Session-Timeout = `%{expr:2 + 3}`
#
#  So the module needs to be instantiated, but CANNOT be
#  listed in any other section.  See 'doc/rlm_expr' for
#  more information.
#
expr
#
# We add the counter module here so that it registers
# the check-name attribute before any module which sets
# it
daily
expiration
logintime
```

Se configura la frase secreta la cual será compartida entre el servidor Freeradius y el punto de acceso inalámbrico. Además se deberá registrar a la dirección IP del punto de acceso inalámbrico asignándole un nombre corto de reconocimiento y la frase secreta para compartir información con el servidor Freeradius.

```
#  The default secret below is only for testing, and should

#  not be used in any real environment.

secret              = ueslg2011

#
#  Clients
#

client 192.168.10.206/24 {

          secret    = ueslg2011

          shortname = puntoacceso

}
```

ARCHIVO DE CONFIGURACIÓN PARA CHILLISPOT (CHILLI.CONF)

En este archivo de configuración de Chillispot, se configura todos los datos descritos en la Tabla 4.1 del tema 4.3.4 Configuración de Chillispot

```
# TUN parameters

# TAG: net

# IP network address of external packet data network

# Used to allocate dynamic IP addresses and set up routing.

# Normally you do not need to uncomment this tag.

#net 192.168.10.0/24

# TAG: dynip

# Dynamic IP address pool

# Used to allocate dynamic IP addresses to clients.

# If not set it defaults to the net tag.
```

Do not uncomment this tag unless you are an experienced user!

#dynip 192.168.182.0/24

TAG: statip

Static IP address pool

Used to allocate static IP addresses to clients.

Do not uncomment this tag unless you are an experienced user!

#statip 192.168.182.0/24

TAG: dns1

Primary DNS server.

Will be suggested to the client.

If omitted the system default will be used.

Normally you do not need to uncomment this tag.

#dns1 200.93.216.2

TAG: dns2

Secondary DNS server.

Will be suggested to the client.

If omitted the system default will be used.

Normally you do not need to uncomment this tag.

#dns2 200.93.216.5

TAG: domain

Domain name

Will be suggested to the client.

Normally you do not need to uncomment this tag.

#domain key.chillispot.org

TAG: ipup

Script executed after network interface has been brought up.

Executed with the following parameters: <devicename> <ip address>

<mask>

Normally you do not need to uncomment this tag.

#ipup /etc/chilli.ipup

TAG: ipdown

Script executed after network interface has been taken down.

Executed with the following parameters: <devicename> <ip address>

<mask>

Normally you do not need to uncomment this tag.

#ipdown /etc/chilli.ipdown

Radius parameters

TAG: radiuslisten

IP address to listen to

Normally you do not need to uncomment this tag.

#radiuslisten 127.0.0.1

TAG: radiusserver1

IP address of radius server 1

For most installations you need to modify this tag.

radiusserver1 127.0.0.1

TAG: radiusserver2

```
# IP address of radius server 2

# If you have only one radius server you should set radiusserver2 to the

# same value as radiusserver1.

# For most installations you need to modify this tag.

radiusserver2 127.0.0.1

# TAG: radiusauthport

# Radius authentication port

# The UDP port number to use for radius authentication requests.

# The same port number is used for both radiusserver1 and radiusserver2.

# Normally you do not need to uncomment this tag.

#radiusauthport 1812

# TAG: radiusacctport

# Radius accounting port

# The UDP port number to use for radius accounting requests.

# The same port number is used for both radiusserver1 and radiusserver2.

# Normally you do not need to uncomment this tag.

#radiusacctport 1813

# TAG: radiussecret

# Radius shared secret for both servers

# For all installations you should modify this tag.

radiussecret ueslg2011

# DHCP Parameters

# TAG: dhcpif
```

```
# Ethernet interface to listen to.

# This is the network interface which is connected to the access points.

# In a typical configuration this tag should be set to eth1.

dhcpif eth1

# TAG: dhcpmac

# Use specified MAC address.

# An address in the range  00:00:5E:00:02:00 - 00:00:5E:FF:FF:FF falls

# within the IANA range of addresses and is not allocated for other

# purposes.

# Normally you do not need to uncomment this tag.

#dhcpmac 00:00:5E:00:02:00

# TAG: lease

# Time before DHCP lease expires

# Normally you do not need to uncomment this tag.

#lease 600

# Universal access method (UAM) parameters

# TAG: uamserver

# URL of web server handling authentication.

uamserver https://192.168.10.87/cgi-bin/hotspotlogin.cgi


# TAG: uamhomepage

# URL of welcome homepage.

# Unauthenticated users will be redirected to this URL. If not specified
```

```
# users will be redirected to the uamserver instead.
# Normally you do not need to uncomment this tag.
uamhomepage http://192.168.10.87/hotspotgonzaga/hotspot.html
# TAG: uamsecret
# Shared between chilli and authentication web server
uamsecret gonzaga
# TAG: uamlisten
# IP address to listen to for authentication requests
# Do not uncomment this tag unless you are an experienced user!
#uamlisten 192.168.182.1
# TAG: uamport
# TCP port to listen to for authentication requests
# Do not uncomment this tag unless you are an experienced user!
#uamport 3990
# TAG: uamallowed
# Comma separated list of domain names, IP addresses or network segments
# the client can access without first authenticating.
# It is possible to specify this tag multiple times.
# Normally you do not need to uncomment this tag.
uamallowed www.uegonzaga.edu.ec
```

ANEXO 2 - REPORTE DE LA BASE DE DATOS RADIUS – TABLA RADACCT

radacctid	username	nasporttype	acctstarttime	acctstoptime	acctsessiontime	acctterminatecause	framedipaddress
1	juan	Wireless-802.11	2011-12-06 08:09:40	2011-12-06 10:19:38	7858	User-Request	192.168.182.2
2	angel	Wireless-802.11	2011-12-06 10:04:11	2011-12-06 11:51:59	6468	User-Request	192.168.182.3
3	paul	Wireless-802.11	2011-12-06 11:28:06	2011-12-06 11:47:37	1161	User-Request	192.168.182.4
4	gperez	Wireless-802.11	2011-12-06 15:07:05	2011-12-06 15:09:06	121	User-Request	192.168.182.2
5	querubin	Wireless-802.11	2011-12-06 15:39:26	2011-12-06 15:43:23	237	User-Request	192.168.182.2
6	angel	Wireless-802.11	2011-12-08 15:22:04	2011-12-08 15:24:59	175	User-Request	192.168.182.2
7	paul	Wireless-802.11	2011-12-08 15:37:51	2011-12-08 15:45:08	437	User-Request	192.168.182.2
8	angel	Wireless-802.11	2011-12-08 16:18:23	2011-12-08 16:19:42	79	User-Request	192.168.182.2
9	juan	Wireless-802.11	2011-12-08 16:24:21	2011-12-08 18:32:13	7672	Lost-Carrier	192.168.182.2
10	lucy	Wireless-802.11	2011-12-09 08:55:31	2011-12-09 13:56:11	18041	User-Request	192.168.182.10
11	juan	Wireless-802.11	2011-12-09 14:03:13	2011-12-09 17:58:09	14097	Lost-Carrier	192.168.182.10
12	angel	Wireless-802.11	2011-12-13 16:28:52	2011-12-13 16:29:30	38	User-Request	192.168.182.2
13	angel	Wireless-802.11	2011-12-13 16:29:48	2011-12-13 16:35:53	365	User-Request	192.168.182.2
14	paul	Wireless-802.11	2011-12-13 16:36:02	2011-12-13 16:36:56	54	User-Request	192.168.182.2
15	paul	Wireless-802.11	2011-12-13 16:37:17	2011-12-13 16:43:41	384	User-Request	192.168.182.2
16	gperez	Wireless-802.11	2011-12-14 07:15:29	2011-12-14 11:04:53	13764	User-Request	192.168.182.2
17	carmen	Wireless-802.11	2011-12-14 11:16:32	2011-12-14 12:08:06	3094	User-Request	192.168.182.2
18	angel	Wireless-802.11	2011-12-14 11:32:14	2011-12-14 12:11:54	2380	User-Request	192.168.182.3
19	cchavez	Wireless-802.11	2011-12-15 08:50:16	2011-12-15 13:15:23	15907	User-Request	192.168.182.2
20	emartinez	Wireless-802.11	2011-12-15 09:26:08	2011-12-15 09:50:11	1443	User-Request	192.168.182.3
21	querubin	Wireless-802.11	2011-12-15 14:30:45	2011-12-15 18:16:45	13560	User-Request	192.168.182.3
22	lucy	Wireless-802.11	2011-12-15 15:00:53	2011-12-15 15:20:32	1179	User-Request	192.168.182.4
23	carmen	Wireless-802.11	2011-12-16 09:12:34	2011-12-16 10:10:37	3483	User-Request	192.168.182.2
24	gperez	Wireless-802.11	2011-12-16 10:56:02	2011-12-16 16:04:39	18517	User-Request	192.168.182.2
25	byron	Wireless-802.11	2011-12-16 12:02:22	2011-12-16 12:14:09	707	User-Request	192.168.182.3
26	juan	Wireless-802.11	2011-12-19 07:36:12	2011-12-19 11:36:49	14437	User-Request	192.168.182.2

27	fabyta	Wireless-802.11	2011-12-19 10:17:07	2011-12-19 12:41:03	8636	User-Request	192.168.182.3
28	emartinez	Wireless-802.11	2011-12-19 10:22:45	2011-12-19 13:06:34	9829	User-Request	192.168.182.4
29	carmen	Wireless-802.11	2011-12-19 11:02:01	2011-12-19 11:20:38	1117	User-Request	192.168.182.5
30	gregory	Wireless-802.11	2011-12-19 15:08:46	2011-12-19 15:47:03	2297	User-Request	192.168.182.2
31	carocuesta	Wireless-802.11	2011-12-19 15:30:23	2011-12-19 16:01:11	1848	User-Request	192.168.182.3
32	paul	Wireless-802.11	2011-12-20 07:42:04	2011-12-20 08:16:39	2075	User-Request	192.168.182.2
33	juan	Wireless-802.11	2011-12-20 08:21:29	2011-12-20 09:02:06	2437	User-Request	192.168.182.2
34	byron	Wireless-802.11	2011-12-20 09:16:34	2011-12-20 16:14:04	25050	User-Request	192.168.182.2
35	cchavez	Wireless-802.11	2011-12-20 13:05:02	2011-12-20 13:06:54	112	User-Request	192.168.182.3
36	lucy	Wireless-802.11	2012-01-03 08:02:53	2012-01-03 12:41:07	16694	User-Request	192.168.182.2
37	emartinez	Wireless-802.11	2012-01-03 10:04:29	2012-01-07 16:54:17	370188	User-Request	192.168.182.3
38	paul	Wireless-802.11	2012-01-03 11:05:34	2012-01-03 14:07:05	10891	User-Request	192.168.182.4
39	byron	Wireless-802.11	2012-01-04 09:45:18	2012-01-04 12:53:02	11264	User-Request	192.168.182.2
40	carmen	Wireless-802.11	2012-01-04 09:51:53	2012-01-04 13:28:04	12971	User-Request	192.168.182.3
41	angel	Wireless-802.11	2012-01-04 10:20:04	2012-01-04 11:30:56	4252	User-Request	192.168.182.4
42	gregory	Wireless-802.11	2012-01-04 10:56:48	2012-01-04 12:06:28	4180	User-Request	192.168.182.6
43	fabyta	Wireless-802.11	2012-01-05 11:38:00	2012-01-05 14:07:32	8972	User-Request	192.168.182.2
44	byron	Wireless-802.11	2012-01-05 11:52:05	2012-01-05 13:09:07	4622	User-Request	192.168.182.3
45	noralama	Wireless-802.11	2012-01-05 13:29:07	2012-01-05 14:29:06	3599	User-Request	192.168.182.3
46	angel	Wireless-802.11	2012-01-05 13:43:16	2012-01-05 16:01:05	8269	User-Request	192.168.182.4
47	juan	Wireless-802.11	2012-01-06 07:52:02	2012-01-06 13:36:14	20652	User-Request	192.168.182.2
48	noralama	Wireless-802.11	2012-01-06 08:21:54	2012-01-06 13:36:23	18869	User-Request	192.168.182.3
49	carocuesta	Wireless-802.11	2012-01-06 08:34:18	2012-01-06 13:36:45	18147	User-Request	192.168.182.4
50	querubin	Wireless-802.11	2012-01-06 09:44:15	2012-01-06 13:36:28	13933	User-Request	192.168.182.5
51	gperez	Wireless-802.11	2012-01-06 09:27:55	2012-01-06 13:37:03	13178	User-Request	192.168.182.6
52	emartinez	Wireless-802.11	2012-01-06 11:39:07	2012-01-06 13:38:19	7152	User-Request	192.168.182.2
53	fabyta	Wireless-802.11	2012-01-06 13:20:29	2012-01-06 16:28:11	11262	User-Request	192.168.182.10